Facultad de Ciencias Económicas y Empresariales, ICADE

Technology and the Future of Work

Autor: Lyons, Clodagh
Coordinadora: Josefina Bengoechea Fernández

MADRID | junio 2022

ÍNDICE DE CONTENIDOS

1. SUMMERY 3
2. RESUMEN 4
3. INTRODUCCIÓN 6
4. JUSTIFICACIÓN DE SU RELEVANCIA 7
5. OBJECTIVO DE LA INVESTIGACIÓN 8
6. METODOLOGÍA 9

REVISIÓN DE LA LITERATURA 10

7. CÓMO LA PANDEMIA CAMBIÓ NUESTRA FORMA DE TRABAJAR 10
8. EL FUTURO DE TRABAJO 16
9. CIBERSEGURIDAD 21
10. ANÁLISIS DE LA INVESTIGACIÓN 25
11. CONCLUSIÓN 39
12. BIBLIOGRAFÍA 41
13. APENDICÉ 44

1. Summery

Technology is much more prominent in workplaces in recent years than it ever has been before. It allows workers to engage in their work even from outside the office thanks to virtual communication means. Technology has consistently made work more accessible and has improved working conditions from the industrial age to the modern day. Advances and technological advantages can be seen across almost every industry. (Grant, 2019)

The benefits of technology were especially highlighted during the global pandemic that took place in 2019 which shook workplaces globally. Organisations being able to continue to work would not have been an option if technology did not exist. Shifting to remote work settings and continuing productivity and active communication was made available through virtual communication which allowed organisations worldwide to connect with one another, independent of where the work was carried out. Although it was a massive adjustment for many initially, it has most definitely transformed the working world. This change in the working environment has become the new norm for many businesses, although tight restrictions and lockdowns have been lifted in the majority of countries. Organisations and employees became accustomed to the many benefits this new work model provided them, especially the increase in flexibility of their working day and an improved work – life balance. Hybrid approaches to work life have become all more common, where workers can carry out their daily tasks from the office or remotely. (Guerra, 2021)

Although there are many benefits, technology also has its challenges and dangers. The biggest threat that companies faced during this shift in work life and through continuous technological advances, was cyberattacks. Entire workforces working from their own spaces leaves organisations much more vulnerable to hackers accessing their data. An increase of cyberattacks occurred due to employees accessing their work from their own networks to carry out their duties. These attacks are becoming all too common and take companies months to recover from them which results in high levels of stress in the organisation and costs high amounts financially to recover the damage. (Irwin, 2021)

Cyber resilience is the ability to prepare, deal with and recover from attacks. It is becoming a main priority within businesses which enable companies to prepare for attacks and even prevent them. (Shemesh, 2022)

Technology helped transform the way we work throughout the pandemic but it is also shaping our future in a completely new way. The increase in robotics in the workplace and the automation of certain jobs will create a different world of work that we have never

experience before. Robots carrying out certain tasks within workplaces is becoming normal and automation of jobs is driving many roles, previously carried out by humans, into extinction. For example, jobs such as book keeping, telemarketing and mathematical technician, to name a few, will all be replaced by automated technology. However, this is not something to fear from, as the removal of these mundane jobs and the implementation of robots into to the workplace will make an organisation more productive creating many new roles for people. (Willems, 2022)

This final degree project is going to focus on how the pandemic changed how we work and how productivity was stabilised in organisations throughout this time. It will also highlight the future possibilities of the workforce and how the introduction of robots into the workplace will change and replace certain jobs that are carried out by humans today. It will go into depth into how technology is driving our future, artificial intelligence in the workforce and how the metaverse could come into existence our future. In this section, it will be underlined how important it is for companies to take technological risks in the future as they will gain a competitive advantage over competing companies that will shy away from adopting new technologies. Lastly cyberattacks and the importance of implementing cybersecurity will be discussed in detail.

The main aim of this project is to highlight how technology is in the core of every industry and job and the effects it has had and will have in the future.

Key terms: *technology, global pandemic, remote working, cyberattacks, cyber resilience, automation, robots*

2. Resumen

En los últimos años, la tecnología está mucho más presente en los lugares de trabajo que antes. Permite a los trabajadores participar en su trabajo incluso desde fuera de la oficina gracias a los medios de comunicación virtuales. La tecnología ha hecho más accesible el trabajo y ha mejorado las condiciones laborales desde la era industrial hasta la actualidad. Los avances y las ventajas tecnológicas pueden verse en casi todos los sectores. (Grant, 2019)

Los beneficios de la tecnología se pusieron especialmente de manifiesto durante la pandemia mundial que tuvo lugar en 2019 y que sacudió los lugares de trabajo a nivel mundial. Que

las organizaciones pudieran seguir trabajando no habría sido una opción si no existiera la tecnología. El cambio a entornos de trabajo remotos y la continuidad de la productividad y la comunicación activa estuvieron disponibles a través de la comunicación virtual, que permitió a las organizaciones de todo el mundo conectarse entre sí, independientemente del lugar donde se realizara el trabajo. Aunque en un principio supuso una gran adaptación para muchos, ha transformado definitivamente el mundo laboral. Este cambio en el entorno de trabajo se ha convertido en la nueva norma para muchas empresas, aunque en la mayoría de los países se han eliminado las restricciones y bloqueos. Las organizaciones y los empleados se han acostumbrado a las numerosas ventajas que les proporciona este nuevo modelo de trabajo, especialmente el aumento de la flexibilidad de su jornada laboral y la mejora del equilibrio entre trabajo y vida privada. Cada vez son más comunes los enfoques híbridos de la vida laboral, en los que los trabajadores pueden realizar sus tareas diarias desde la oficina o a distancia. (Guerra, 2021)

Aunque hay muchos beneficios, la tecnología también tiene sus retos y peligros. La mayor amenaza a la que se enfrentaron las empresas durante este cambio en la vida laboral y gracias a los continuos avances tecnológicos, fueron los ciberataques. El hecho de que fuerzas laborales enteras trabajen desde sus propios espacios deja a las organizaciones mucho más vulnerables a que los hackers accedan a sus datos. El aumento de los ciberataques se debe a que los empleados acceden a su trabajo desde sus propias redes para realizar sus tareas. Estos ataques se están convirtiendo en algo demasiado común y las empresas tardan meses en recuperarse de ellos, lo que provoca un alto nivel de estrés en la organización y un elevado coste económico para recuperar los daños. (Irwin, 2021)

La resiliencia cibernética es la capacidad de prepararse, afrontar y recuperarse de los ataques. Se está convirtiendo en una prioridad principal dentro de las empresas que les permite prepararse para los ataques e incluso prevenirlos. (Shemesh, 2022)

La tecnología ayudó a transformar la forma de trabajar durante la pandemia, pero también está dando forma a nuestro futuro de una manera completamente nueva. El aumento de la robótica en el lugar de trabajo y la automatización de ciertos trabajos crearán un mundo laboral diferente que nunca hemos experimentado. Que los robots realicen ciertas tareas en los lugares de trabajo se está convirtiendo en algo normal y la automatización de los puestos de trabajo está llevando a la extinción muchas funciones que antes realizaban los humanos. Por ejemplo, trabajos como la teneduría de libros, el telemarketing y el técnico matemático, por nombrar algunos, serán sustituidos por tecnología automatizada. Sin embargo, esto no es algo que deba temerse, ya que la eliminación de estos trabajos mundanos y la

implantación de robots en el lugar de trabajo hará que una organización sea más productiva, creando muchas nuevas funciones para las personas. (Willems, 2022)

Este proyecto de fin de carrera se va a centrar en cómo la pandemia cambió la forma de trabajar y cómo se estabilizó la productividad en las organizaciones durante todo este tiempo. También destacará las posibilidades futuras de la mano de obra y cómo la introducción de los robots en el lugar de trabajo cambiará y sustituirá ciertos trabajos que hoy realizan los humanos. Se profundizará en cómo la tecnología está impulsando nuestro futuro, la inteligencia artificial en la fuerza de trabajo y cómo el metaverso podría llegar a existir nuestro futuro. En este apartado se destacará la importancia de que las empresas asuman riesgos tecnológicos en el futuro, ya que obtendrán una ventaja competitiva frente a las empresas competidoras que rehúyen la adopción de nuevas tecnologías. Por último, se analizarán en detalle los ciberataques y la importancia de aplicar la ciberseguridad.

El objetivo principal de este proyecto es poner de manifiesto cómo la tecnología está en el centro de todas las industrias y trabajos y los efectos que ha tenido y tendrá en el futuro.

Términos clave: *tecnología, pandemia mundial, trabajo a distancia, ciberataques, ciberresistencia, automatización, robots*

3. Introducción

La pandemia de coronavirus o Covid-19 ha cambiado sin duda la forma de trabajar de las multinacionales y de la mano de obra en general y ha tenido que remodelar la movilidad humana en todo el mundo. La idea de sentarse junto a los compañeros en una oficina abarrotada, de viajar por trabajo o de tener reuniones cara a cara se ha visto alterada desde principios de la década de 2020. Se introdujo la idea del trabajo a distancia o el modelo de "trabajo desde casa", una idea ajena a la mayoría en ese momento. La pandemia mundial puso a disposición condiciones de trabajo flexibles, permitiendo a los empleados elegir su lugar de trabajo. Las videoconferencias se convirtieron en la nueva normalidad y adaptar los horarios de trabajo para conectarse con los que estaban al otro lado del globo era algo que los trabajadores tenían que aceptar. (Enache & Puscas, 2020)

La adopción de las nuevas tecnologías fue vital para la implantación del modelo de "trabajo desde casa". La confianza entre empleadores y empleados se hizo más importante y la idea de las violaciones de datos y la piratería de los sistemas se hizo más común. En general, la

continuidad de la jornada laboral en estos tiempos difíciles no habría sido posible sin la tecnología.

4. Justificación de su relevancia

La tecnología da forma a la empresa moderna y al funcionamiento de todos los procesos de la organización. Sea cual sea el tamaño de la empresa, la tecnología proporciona a las empresas ingresos tangibles e intangibles y quienes invierten en la mejor tecnología obtendrán mayores beneficios. La infraestructura tecnológica también puede influir en las relaciones comerciales, la cultura de la empresa y la eficiencia de la misma. Cuando la tecnología se utiliza correctamente, proporciona a las empresas una productividad óptima. También añade seguridad a las empresas en la actualidad, que es uno de los aspectos más importantes que las empresas deben tener en cuenta. (Kokemuller, 2019)

Este trabajo de investigación analiza en profundidad la adaptación del trabajo en una oficina al trabajo a distancia, los efectos de la pandemia en los lugares de trabajo y la importancia de la tecnología en la actualidad. Asimismo, se analiza el futuro de lo que pueden ser nuestros lugares de trabajo y los puestos de trabajo que pueden existir o no en el futuro del mundo empresarial. También profundiza en los riesgos que puede conllevar el aumento del uso de la tecnología en las empresas, como la piratería de los sistemas y los ataques a la ciberseguridad, así como la importancia que tiene la ciberresiliencia en las estructuras organizativas actuales.

Este tema es extremadamente relevante en el mundo laboral actual y en el futuro de las empresas. La pandemia mundial sin precedentes afectó a todo el mundo, en su vida personal y profesional. Planteó muchos retos a las organizaciones, que tuvieron que adaptarse rápidamente a una nueva forma de trabajar, al tiempo que garantizaban la ciberseguridad de su empresa durante todo este proceso. El aumento de la implantación de la robótica en el lugar de trabajo se produce a diario y la automatización de los puestos de trabajo actuales va en aumento. Los empleados están empezando a reciclarse y a reciclar sus conocimientos para estar en consonancia con el futuro de nuestro trabajo. Adoptar las nuevas tecnologías en una época en la que los cambios se suceden con rapidez es muy importante para que las empresas se aseguren de mantener su ventaja competitiva. Este trabajo de investigación explicará que si las organizaciones no se mueven al mismo ritmo que los cambios tecnológicos, se quedarán atrás.

5. Objectivo de la investigación

Este trabajo de investigación aborda el cambio en la forma de trabajar de las organizaciones debido a las repercusiones de la pandemia mundial, pero también a los continuos avances tecnológicos. El objetivo principal del documento es ofrecer al lector un análisis en profundidad de las ventajas y los retos que estos cambios han aportado al lugar de trabajo y seguirán aportando en el futuro. Teniendo en cuenta que los desarrollos y las alteraciones que la pandemia mundial ha traído al lugar de trabajo constituyen el núcleo de este trabajo de investigación, es esencial establecer primero los objetivos que se pretenden alcanzar.

El objetivo de la primera sección del documento es ofrecer un análisis teórico y estadístico de cómo la pandemia mundial y la tecnología han cambiado la mano de obra y cómo puede ser el futuro del trabajo. El documento comenzará proporcionando al lector un análisis en profundidad de cómo las empresas pasaron de trabajar en la oficina a trabajar a distancia debido al COVID-19. El documento pretende retratar si los niveles de productividad aumentaron o disminuyeron a lo largo de este tiempo y las variables que hay que tener en cuenta para medirlo. Además, ofrecerá un análisis sobre si el trabajo a distancia y el trabajo flexible han llegado para quedarse después de la COVID. El documento también proporcionará al lector un informe en profundidad sobre los puestos de trabajo que se crearon durante los dos años de la pandemia o sobre cómo la pandemia demostró la importancia de algunas funciones sobre otras.

Asimismo, ofrecerá al lector una visión de las predicciones sobre cómo cambiará la tecnología en el futuro y modificará por completo nuestra forma de trabajar. Se explicará cómo se automatizarán los puestos de trabajo y el impacto de la introducción de robots en el lugar de trabajo. ¿Suprimirá necesariamente puestos de trabajo o creará una multitud de nuevos empleos para las generaciones futuras?

El objetivo del artículo es mostrar los beneficios de la tecnología, pero también el aumento del riesgo. El lector comprenderá cómo el aumento de la tecnología en las plantillas, especialmente durante el aumento de la capacidad de trabajar desde casa durante la pandemia, ha provocado ciberataques. Sin embargo, el objetivo es exponer claramente al lector las estrategias puestas en marcha por las empresas en los últimos años para reducir estos riesgos y cómo se pueden prevenir los ciberataques en el futuro.

A continuación, se analizan las entrevistas realizadas. Los entrevistados trabajan en empresas globales de diferentes sectores, desde las tecnologías de la información hasta la contratación y la seguridad. El objetivo de esta sección del documento es que los entrevistados compartan sus experiencias personales sobre las cuestiones señaladas anteriormente y se realizará un análisis exhaustivo de sus experiencias. Esta parte informará al lector de los impactos personales que el trabajo a distancia les ha causado, si la productividad aumentó durante la pandemia y si quieren que el trabajo a distancia se mantenga. También se explicará su experiencia con la automatización de la mano de obra, cómo ha cambiado la naturaleza de su trabajo debido a la tecnología y cómo esperan que evolucione. Por último, se analizarán las principales estrategias puestas en marcha por sus respectivas empresas para garantizar su ciberresistencia.

La comparación de estas dos secciones me permitirá llegar a una conclusión práctica.

6. Metodología

En la primera sección de este proyecto de fin de carrera se emplea un enfoque de investigación inductiva. Para esta sección del proyecto se sigue un examen exhaustivo de la literatura preexistente. Para la segunda sección, se recopiló información mediante la realización de entrevistas con personas que trabajan en diferentes organizaciones tanto en Irlanda como en España. Para analizar esta segunda sección, se recogió y analizó la investigación cualitativa utilizando un enfoque interpretativo. Como investigador de este estudio, mi percepción de los datos que he recogido puede influir en los resultados obtenidos.

En la primera sección, se realizó una revisión colectiva de la literatura existente. Para ello se leyeron e investigaron recursos académicos, revistas, artículos y recursos proporcionados por académicos de todo el mundo con información experta sobre los temas investigados. En este estudio se incluyen las investigaciones relacionadas con la forma en que la tecnología impulsa nuestro trabajo, la creación de nuevos puestos de trabajo y la ciberseguridad. La información de estas fuentes se encontró a través de informes tecnológicos realizados por organizaciones tecnológicas globales como Deloitte, Accenture y McKinsey&Company.

También Google Scholar fue un sistema de información vital utilizado a lo largo de este trabajo de investigación y proporcionó referencias y fuentes de información fiables.

La segunda sección del documento utiliza únicamente fuentes primarias. Se realizaron entrevistas a lo largo de este estudio para obtener experiencias de la vida real e información que pudiera respaldar mi investigación secundaria. La naturaleza de este tema es sorelevante en nuestra sociedad actual, ya que la pandemia mundial y la tecnología han afectado a la vida personal y profesional de todos. Por lo tanto, las entrevistas fueron el enfoque más adecuado para llevar a cabo mi investigación y análisis. Se entrevistó a seis candidatos, todos ellos con diferentes funciones, como tecnologías de la información, consultoría, gestión de la producción, contratación, seguridad y ética y cumplimiento. El hecho de contar con un abanico tan amplio de funciones me permitió conocer a fondo cómo la pandemia mundial ha alterado el lugar de trabajo y cómo la tecnología ha hecho cambiar sus funciones. Las entrevistas se realizaron por teléfono o mediante videollamadas que luego transcribí para analizarlas. Las entrevistas se añadirán en su forma original al final de este trabajo de investigación. A lo largo de esta parte del trabajo se ha utilizado un análisis interpretativo.

Revisión de la literatura

7. Cómo la pandemia cambió nuestra forma de trabajar

7.1 La eficacia del trabajo a distancia

Ahora que llevamos más de dos años de pandemia mundial, se plantea la cuestión de la eficacia real del trabajo a distancia.

Con la reapertura de las economías, los enfoques híbridos están definitivamente aquí para quedarse para muchos en el mundo corporativo. Esto se debe a que la naturaleza del trabajo a distancia y la capacidad de trabajar desde el espacio elegido han roto muchas barreras en términos de tecnología y cultura y, de hecho, han abierto muchas más opciones para las personas en términos de empleo. Para otros, no podían trabajar a distancia en absoluto. Los empleadores de ciertos sectores han descubierto que ahora tienen la opción y la capacidad de adaptarse al trabajo a distancia en términos de crisis, pero creen que los niveles de productividad y el trabajo se realizan más eficazmente en persona.

Se trataría de actividades como el coaching, el asesoramiento y la provisión de consejos y retroalimentación. Además, es más eficaz entablar relaciones entre clientes y colegas en persona, así como, incorporar a nuevos empleados a una empresa, negociar y tomar decisiones cruciales, enseñar y formar y, por último, el trabajo de colaboración. (Madgavkar, et al., 2020)

En cuanto a la productividad entre el trabajo en la oficina y el método de trabajo desde casa, hay que tener en cuenta muchos datos demográficos diferentes. Entre ellos, el género, la edad y los ingresos. (Santana y Cobo, 2020)

Se presume que los hombres serían más productivos que las mujeres con la visión tradicional de que las mujeres tienen más tareas domésticas o de cuidado de los niños en comparación con los hombres. Sin embargo, las investigaciones realizadas a lo largo de la pandemia han concluido que los niveles de productividad son los mismos dentro de estas brechas de género, si no que los niveles de productividad han sido más producidos por las mujeres. (Awada et al.)

Además, con respecto a los ingresos y la edad, se dice que los que tienen más antigüedad y un salario más alto tienden a ser más productivos que los que son más jóvenes y tienen un nivel de ingresos más bajo. (Feyrer), (Roosaar et al.)

También hay que tener en cuenta el ejemplo de los trabajadores de mediana edad que tienen responsabilidades familiares, como trabajar junto a sus hijos u otros miembros de la familia, y que podrían verse abrumados y tener más dificultades para equilibrar sus tareas. (Gorlick, 2020)

En función de las diferentes ocupaciones, como he mencionado anteriormente, se dice que los trabajadores cuyo trabajo está rodeado principalmente de estaciones de trabajo informáticas (por ejemplo, los programadores) han tenido más productividad en la transición de trabajar en un espacio de oficina a trabajar desde casa. (Awada et al.)

Otro factor sería la salud de los trabajadores, el empeoramiento de los factores de salud como la fatiga ocular, el cansancio y el dolor de cabeza debido al mayor tiempo que se pasa mirando las pantallas también ha disminuido la productividad. Además, un aumento de los problemas de salud mental, como la ansiedad, la depresión, el insomnio y el estrés, puede disminuir aún más la productividad de algunos trabajadores. (Goetzel et al.)

Otro aspecto a tener en cuenta es, de hecho, el espacio que el empleado ha elegido para realizar su trabajo a distancia. La transición de trabajar en un espacio de oficina establecido a una habitación en la propia vivienda puede resultar un reto para muchos. Es muy importante que los trabajadores elijan un entorno en el que se sientan cómodos y libres de distracciones a la hora de realizar esta rápida adaptación. En algunos casos, es inevitable que las personas tengan que compartir espacios de trabajo cuando se adaptan a su entorno de trabajo a distancia debido a la limitación de espacio en su vivienda.

Una encuesta realizada por Suart et al. concluyó que sólo el 48,6% de los encuestados tenía un espacio de trabajo dedicado y adecuado, el 31% tenía un espacio de trabajo compartido con otras personas y el 20,4% trabajaba en diferentes zonas de su casa.

Aunque la idea inmediata es que el 20,4% restante que disponía de espacios de trabajo ajustables podría demostrar una mayor improductividad, en realidad, la falta de capacidad para cambiar el espacio de trabajo de uno mismo dio lugar a niveles de productividad más bajos. Una encuesta llevada a cabo por Rudnicka et al. demostró que los encuestados se sentían más productivos y observaban un mayor rendimiento laboral cuando tenían la libertad de ajustar su espacio de oficina con regularidad. (Awada et al.)

Los factores que crean estas condiciones de trabajo favorables son el acceso a la luz natural y la calidad del ambiente interior, como la ventilación, la calidad del aire y el control de la temperatura. (Awada y Srour) Se ha comprobado que el mayor acceso a la luz natural no sólo aumenta el rendimiento de los trabajadores en un 13%, sino que también reduce la fatiga del empleado. (Heschong et al.) En todas las investigaciones realizadas dentro del tema de la productividad y el espacio de trabajo elegido, se dice que cuando los individuos tienen el control del lugar donde pueden trabajar se sienten mucho más satisfechos con su trabajo y esto a su vez aumenta la productividad de los trabajadores.

Siguiendo con la productividad del método de trabajo desde casa, otro aspecto a tener en cuenta son los límites que los trabajadores establecen y mantienen dentro de su oficina en casa; límites entre las tareas del trabajo y las responsabilidades del hogar. El equilibrio entre las tareas del hogar y las del trabajo siempre ha sido una tarea conflictiva que hay que equilibrar, incluso antes de la pandemia. (Shaffer et al.),(Hunter et al.) Pero el modelo de trabajo desde casa lo ha hecho mucho más difícil para algunos, lo que significa que muchos tienen que ajustar su horario de trabajo. Muchos se acogen a la libertad de la flexibilidad

que aporta la situación de trabajo a distancia, mientras que otros simplemente tienen que trabajar en torno a sus obligaciones domésticas, lo que significa que podrían tener que trabajar en horas intempestivas, como por ejemplo a primera hora de la mañana, a última hora de la noche y durante todo el fin de semana. (Awada et al.)

Como estas responsabilidades no afectan a todas las personas en el lugar de trabajo, puede haber un aumento de las expectativas laborales para las que tienen estas responsabilidades adicionales. Debido a las mayores expectativas, es posible que se espere que los trabajadores realicen más tareas que antes y entreguen trabajo adicional. Esto, a su vez, aumenta sus horas de trabajo y prolonga su tiempo en su puesto de trabajo. (Singh et al.)(Balkeran)

En general, Ctrip llevó a cabo un estudio basado en 1.000 empleados de una empresa de viajes china y, en total, hubo un aumento del 13% en los índices de productividad gracias al trabajo a distancia. Además, hubo casi un día más de producción por semana y un descenso del 50% en las tasas de abandono de los empleados (Gorlick, 2020).

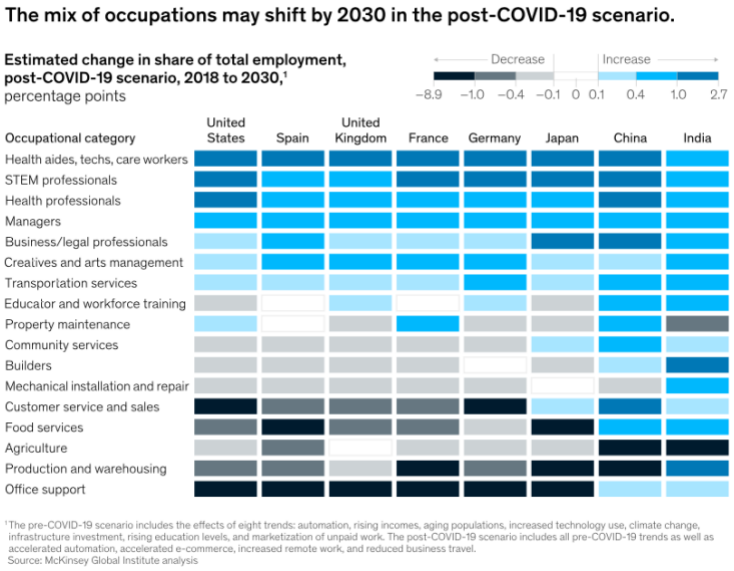
7.2 Cómo la pandemia cambió la forma de trabajar y la creación de nuevos empleos

La pandemia cambió la forma de trabajar de muchas personas y ajustó su visión de lo que debe ser un lugar de trabajo. En primer lugar, según un informe publicado por deloitte llamado "COVID-19 como catalizador" ha mencionado que las nuevas formas de trabajo virtual han desbloqueado las oportunidades de innovación en el lugar de trabajo. Una encuesta realizada en este estudio ha destacado los resultados de que tanto los líderes como los empleados están encontrando que el trabajo virtual les ofrece nuevas formas de trabajar y de ver la innovación. Una de las principales constantes durante los tiempos sin precedentes y el paso al trabajo a distancia fue la urgencia en la toma de decisiones operativas, clínicas y financieras y cómo los CHROs obligaron a sus organizaciones a acelerar y cambiar sus procesos de toma de decisiones. Este cambio obligó a los equipos a elaborar o ajustar los planes con rapidez y llevó a establecer comunicaciones más significativas y frecuentes y a encontrar nuevas formas de interactuar entre sí. Celebraban más reuniones con los empleados para determinar sus metas y objetivos en un proyecto, lo que potenciaba un trabajo más eficaz. Empezaron a centrarse más en la microgestión, lo que también dio lugar a una aceleración de los procesos de toma de decisiones y minimizó o eliminó por completo las tareas de poco valor.

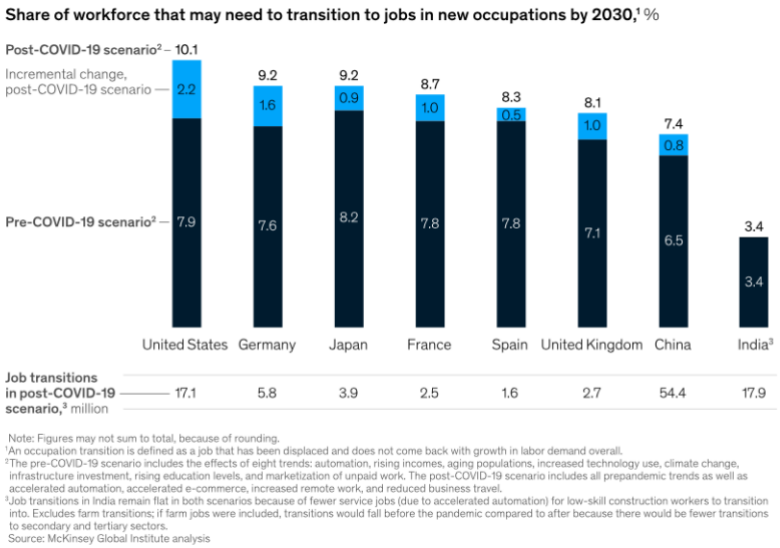
El cambio al trabajo a distancia también dio a las organizaciones la oportunidad de explorar nuevas tecnologías y el cambio a las reuniones virtuales estimuló los avances en la transformación digital para muchos. Por ejemplo, los responsables de la sanidad estaban implementando "chat bots" para atender mejor a los pacientes. Otro ejemplo que dio a los trabajadores la sensación de que seguían trabajando juntos en el entorno de la oficina (aunque lo hicieran a distancia) fue la implantación de la realidad aumentada (RA). Podían crear sus propios avatares, lo que les proporcionaba la experiencia de estar juntos en una sala, permitiéndoles ver el lenguaje corporal de los avatares de sus compañeros de trabajo, los movimientos de las manos, e incluso detectar el contacto visual y si ese empleado estaba prestando atención. (Radin & Korba, 2020)

En cuanto a los trabajos físicos, es justo decir que la pandemia ha cambiado la naturaleza de muchos trabajos y ha demostrado a mucha gente qué trabajos se consideran esenciales, al tiempo que ha aclarado los trabajos que pueden no ser tan necesarios. Se prevé que los puestos de trabajo en el sector alimentario, las funciones de servicios y atención al cliente y las funciones de apoyo a la oficina menos cualificadas sean los que más rápidamente disminuyan. Sin embargo, durante la pandemia, se han creado más puestos de trabajo en el sector del transporte y el almacenamiento, debido al crecimiento del comercio electrónico y la economía de reparto. Sin embargo, se dice que el aumento de estos puestos de trabajo no va a perturbar los empleos con salarios más bajos. Un ejemplo que lo demuestra es el de Estados Unidos, donde se prevé que los puestos de trabajo en el sector de la atención al cliente y los servicios de alimentación se reduzcan en 4,3 millones, mientras que el sector del transporte aumentará en 800.000.

La mayor atención a la salud a lo largo de la pandemia podría hacer que las ocupaciones sanitarias y STEM crecieran, así como sus ingresos en estos empleos. (Lund, et al., 2021)



En las ocupaciones con salarios altos, se espera que estas oportunidades de trabajo crezcan mucho más que las ocupaciones con salarios bajos. Se prevé que estas transiciones en la mano de obra sean un reto, ya que, según una investigación realizada por McKinsey & Co. centrada en ocho países, 1 de cada 16 trabajadores tendrá que encontrar una nueva ocupación para 2030. Esto supone un 12% más de lo que se esperaba antes de la pandemia. Además, esta cifra es un 25% mayor en las economías más avanzadas. (Lund, et al., 2021)



8. El Futuro de Trabajo

8.1 El futuro de trabajo

Se prevé que durante los próximos 18 a 24 meses, las organizaciones comenzarán a explorar más oportunidades. Las empresas pueden "crear capacidades de intercambio de datos seguras y sin fisuras que les ayuden a rentabilizar sus propios activos de información y a alcanzar objetivos empresariales utilizando los datos de otras personas". (deloitte tech trends 2022: Data sharing made easy)

Según el informe Deloitte Tech Trends 2022, tampoco se sabe con exactitud qué deparará el futuro a los lugares de trabajo. Sin embargo, es inevitable que la innovación tecnológica se produzca constantemente a gran velocidad y que los robots estarán presentes en las plantillas futuras con toda seguridad. Creen que la única manera de tener éxito en el lugar de trabajo en el futuro, es estar entusiasmado y dispuesto a adoptar estas nuevas tecnologías. Los humanos van a tener que adaptarse a una vida laboral en la que humanos y robots trabajen juntos. (Bechtel y Buchholz, 2022) (Coros, 2019)

Sin duda, la automatización está reconfigurando los lugares de trabajo, pero ¿es necesario que no haya puestos de trabajo para nosotros en el futuro?

Como sabemos, la implantación de robots en el lugar de trabajo aumentará la eficiencia de algunos trabajos y la calidad del trabajo realizado, y reducirá los costes laborales, pero al mismo tiempo creará más puestos de trabajo para sus homólogos humanos. Deloitte ya ha realizado una encuesta entre los responsables de TI e ingeniería y los resultados son que el 74% de los encuestados ha comprobado que la adopción de la automatización en la plantilla ha aumentado la eficiencia. Además, el 59% afirma que se ha producido una importante reducción de costes y también un aumento de la seguridad. Debido a estas ventajas, el 95% de los encuestados ha dado prioridad a los robots en el lugar de trabajo, mientras que el 21% dice que es una gran prioridad. La implantación de robots en el lugar de trabajo también puede ayudar a los trabajadores a mejorar su cualificación en lugar de tener que perder su empleo. (Los robots y tu trabajo: cómo la automatización está cambiando el lugar de trabajo, 2021)(Coros, 2019) (Bechtel y Buchholz, 2022).

Una teoría que explica por qué los robots realmente aumentan el empleo es que una empresa que adopta robots se vuelve mucho más productiva y realmente necesita humanos para

satisfacer su mayor demanda en la producción. Además, el cerebro humano tiene que interferir en el trabajo de los robots y explicar las emociones y la psicología de los clientes. Por ejemplo, analizar las tendencias de los consumidores. Tradicionalmente se ha dicho que la IA en robótica es incapaz de diferenciar entre "...las conexiones estadísticas significativas y las que no lo son". (Bechtel y Buchholz, 2022) Sin embargo, se dice que crean más trabajo para los empleos menos cualificados, como los empaquetadores de cajas, así como para los trabajadores más cualificados, como los ingenieros. Esto significa que los trabajadores de cualificación media son los que más riesgo corren de perder sus puestos de trabajo a causa de la automatización.

Sin embargo, las máquinas han crecido recientemente de forma exponencial en cuanto a su potencia y capacidades. Ahora están siendo diseñadas para tener cierto nivel de agudeza emocional que borra la tradicional jerarquía cognitiva humano-máquina. Las aplicaciones de IA están empezando a ser entrenadas por los investigadores para ser más versátiles y orientadas al detalle de una manera humana. Ya se pueden ver ejemplos de esto en los centros de llamadas a clientes, bancos y restaurantes con las interacciones extremadamente parecidas a las humanas que realizan los bots de IA. Una idea de lo que puede desarrollarse como siguiente paso de esta tecnología de partida es que un bot de IA diferencie la caída de un objeto en comparación con la de un humano que se ha caído y ahora necesita ayuda.

Si la IA sigue creciendo de la forma exponencial que lo está haciendo en términos de capacidades emocionales, la próxima década podría traer bots que trabajen como educadores, escritores, médicos y jefes de información (Bechtel y Buchholz, 2022).

Hay un estudio realizado por la profesora de operaciones Lynn Wu y el profesor de emprendimiento y gestión Bryan Hong titulado "The Robot Revolution: Consecuencias gerenciales y laborales para las empresas". Los datos de su estudio revelaron que, de hecho, se produjo una pérdida de empleo en las empresas que no han adoptado la automatización, ya que son menos productivas en relación con sus competidores que han adoptado esta tecnología. Por lo tanto, las empresas que no adoptaron la tecnología tuvieron que despedir a más trabajadores.

El único efecto negativo que podrían tener los robots sobre los empleados de una empresa es que pueden hacer que los directivos se vuelvan un poco innecesarios. Esto se debe a que, a medida que se adapta esta moderna tecnología, aumenta la eficiencia del trabajo y se

reducen drásticamente los resultados de los errores humanos. Esto implica que se necesita poca supervisión por parte de los directivos.

Como se ha mencionado anteriormente, el crecimiento de los puestos de trabajo no es uniforme, por lo tanto, el tipo de gestores que se necesitan en el lugar de trabajo será muy diferente. Se necesitarán más gestores para los trabajadores poco cualificados y para los altamente cualificados, pero menos para los que están en el medio.

Algunas diferencias y avances que tendrán los directivos es que podrán gestionar a muchos más trabajadores debido a la adopción de robots que aumentan la estandarización y la eficiencia. Pero para los que están a cargo de trabajadores de alta cualificación, es más difícil medir la innovación y, al estar tan cualificados, a menudo no necesitan un gestor. Los directivos más cualificados tienden a actuar más como entrenadores o asesores de los trabajadores que a supervisarlos. (Los robots y tu trabajo: cómo la automatización está cambiando el lugar de trabajo, 2021)

8.2 La Inteligencia Artificial y cómo la tecnología está dando forma a nuestro futuro

La Inteligencia Artificial se define "generalmente como la capacidad de una máquina de realizar funciones cognitivas tan bien o mejor que los humanos". Estas funciones pueden incluir cosas como la percepción, el aprendizaje, la resolución de problemas, el razonamiento, la realización de predicciones y el ejercicio de la creatividad. El uso de la Inteligencia Artificial puede emplearse en la mayoría de las industrias y puede utilizarse para un sinfín de operaciones como la resolución de problemas empresariales, puede detectar el fraude, gestionar las cadenas de suministro, recomendar productos e incluso puede servir de ayuda a los escritores en su trabajo. Estas funciones son sólo para nombrar algunas. La forma en que la inteligencia artificial supuso una ventaja para la industria de la salud a lo largo de la pandemia fue que automatizó el proceso de descubrimiento de fármacos, lo que a su vez condujo a las posibilidades de la vacuna COVID-19. (Webb, 2022)

Voy a centrarme en la industria del consumo y describir cómo la implantación de la IA la está transformando. Como ya se ha mencionado, la IA es ahora capaz de detectar las emociones, así como de simular la empatía y la emoción. Un equipo de la Universidad Queen Mary de Londres realizó pruebas para comprobar lo bien que la IA podía detectar

diferentes emociones como el miedo, el asco, la alegría y la relajación. La máquina tuvo una precisión del 71% en estas pruebas, lo que significa que esta maquinaria puede utilizarse en aplicaciones de salud y bienestar, pero también en procesos como las entrevistas de trabajo y la inteligencia militar. Tecnologías como ésta van a marcar nuestro futuro hasta el punto de que incluso una entrevista no requiera mano de obra.

En cuanto a la inteligencia artificial, estar equipada para detectar con precisión el estado empático y emocional de una persona se considera una tarea más difícil, pero aún así la han superado. Las empresas que disponen de conjuntos de datos lo suficientemente grandes están desarrollando modelos precisos de esta IA. Un ejemplo donde se utilizan estos sistemas es en el sector de la automoción. Utilizan la tecnología diseñada por “Affectiva”. “Affectiva” tiene una IA que puede utilizar el análisis del habla, la visión por ordenador y la visión profunda para analizar estados humanos complejos. Las industrias de la automoción emplean esta tecnología para detectar diferentes estados emocionales en los conductores, como la rabia en la carretera o la somnolencia, y dar sugerencias en el momento que puedan afectar positivamente a su conducción. (Webb, 2022)

En el futuro se dice que las máquinas serán capaces de sentir emociones humanas como el miedo, el amor, la tristeza y la felicidad. De nuevo, es difícil tener una emoción concreta para éstas debido a la complejidad del cerebro humano y a cómo registra las emociones de forma diferente. Hay una teoría que da la capacidad de imaginar el estado mental de otra persona que se conoce como "Teoría de la Mente". La forma en que los investigadores de IA están combatiendo el reto de permitir que las máquinas registren diferentes emociones es entrenándolas para que construyan su propio modelo de teoría de la mente. Si esto tiene éxito, esta tecnología podría utilizarse para la terapia y los asesores de salud mental. Estas máquinas y tecnologías podrían acabar en escuelas, hospitales, prisiones y otras instituciones para ofrecer apoyo emocional a través de bots personales a pacientes y estudiantes. También esta podría ser la respuesta futura a quienes sufren altos niveles de soledad, el apoyo emocional será ofrecido por bots en lugar de personas. (Webb, 2022)

La forma en que la tecnología está dando forma a nuestro futuro está empezando con los avances en la Inteligencia Artificial, sin embargo, creciendo sobre esto está la idea del "Metaverso" que se define como un "futuro de ciencia ficción de un espacio de realidad virtual persistente y compartido" en la "Visión Tecnológica 2022" de “Accenture.” El metaverso se está construyendo ahora abordando diferentes enfoques e ideas y encontrando

la solución para hacerlo bien. Algunos ángulos son para los consumidores mientras que otros se centran en las empresas, sin embargo, cada idea tiene una plataforma diferente, diferentes socios y tecnologías en su núcleo.

Aunque esto parece poco realista en este momento, “Accenture” lo compara con la rapidez con la que evolucionó Internet, empezando por simples sitios web hasta ser el núcleo de la mayoría de los negocios en el mundo actual.

El metaverso está evolucionando y expandiéndose en múltiples dimensiones:

1. Se trata de un compromiso de múltiples tecnologías que incluyen la realidad extendida, la inteligencia artificial, la cadena de bloques, los gemelos digitales y los objetos inteligentes, como los coches y las fábricas.
2. Lleva la "virtual-realidad" a un nuevo nivel y mezcla experiencias virtuales y físicas.
3. Reimagina y transforma las experiencias de los consumidores, las aplicaciones y los modelos de negocio de las empresas. (Carrel - Billiard et al., 2022)

Se dice que "el 98% de los ejecutivos cree que los continuos avances tecnológicos son más fiables que las tendencias económicas, políticas o sociales a la hora de informar sobre la estrategia a largo plazo de sus organizaciones".

Ya hay ejemplos del metaverso en acción, como una redacción virtual con presentadores de IA en China que puede ofrecer noticias de última hora a cualquier hora del día. Esto demuestra que estamos entrando en un nuevo paisaje en el que no existen reglas ni expectativas, lo que genera una gran cantidad de oportunidades para desarrollar y dar forma a los mundos del mañana.

Las empresas que despliegan estos bots de tipo humano, como se ha mencionado anteriormente, no sólo obtienen los beneficios de la automatización, sino que crean formas mejoradas de colaboración entre humanos y máquinas. La transformación de los materiales inteligentes y las capacidades de borde están a un ritmo que se espera de los entornos físicos. Las empresas que venden artículos en el metaverso suministran productos fundamentalmente diferentes, y también están probando nuevas modalidades de comercio y desarrollando las mejores prácticas para el futuro de Internet. Las empresas que ya están construyendo y mejorando en estos nuevos mundos que se están creando reciben nuevas ideas y criterios que configuran el futuro próximo de cómo vivirán las personas, dónde

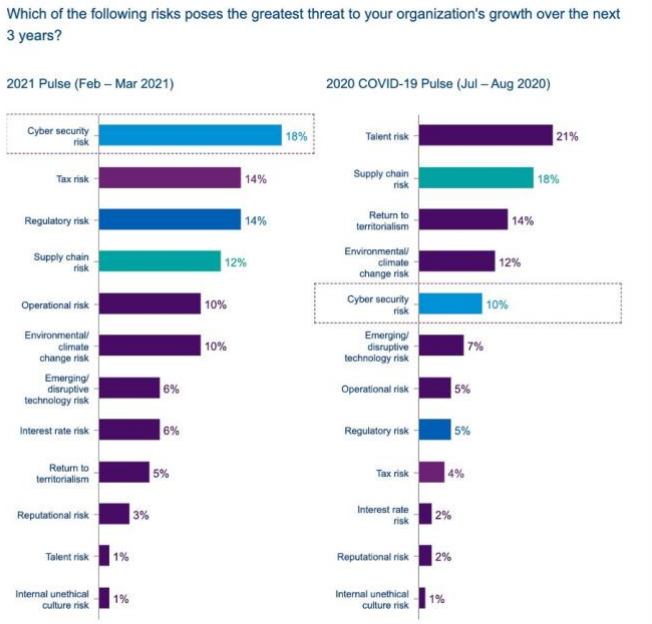
pueden encontrar oportunidades las empresas y la importancia de ser una organización responsable dentro de estos nuevos entornos. (Carrel - Billiard et al., 2022)

La tecnología está evolucionando y está dando forma al cambio para el futuro. Según Peter Ducker, "La mejor manera de predecir el futuro es crearlo". (Bechtel, et al., 2020) Esta cita es exactamente lo que está ocurriendo, si las empresas y organizaciones no se adaptan y evolucionan con este rápido crecimiento de la innovación tecnológica, perderán muy rápidamente cualquier ventaja competitiva. Según el informe de Accenture Technology, dicen que aquellas empresas que se aparten de este nuevo mundo se encontrarán en situaciones en las que están trabajando en mundos que ya han sido definidos, básicamente "jugando con las reglas de otros". Sin embargo, aquellas empresas que estén dispuestas a arriesgarse verán el metaverso como una oportunidad y abrazarán la incertidumbre. En realidad, este nuevo mundo tecnológico redefinirá todo el contexto empresarial, influyendo en la forma en que las empresas operan y producen valor durante las próximas décadas. Este es el futuro y el hecho de que las empresas se abstengan de entrar en él no impedirá que se produzca. Los primeros cimientos del metaverso se están construyendo y aquellos que se arriesguen a tomar posiciones y alianzas, mientras siguen invirtiendo en tecnología, obtendrán un liderazgo temprano en este nuevo mundo. Sin embargo, este nuevo mundo sigue planteando muchos interrogantes, ya que está lleno de incertidumbre y va más allá de las zonas de confort de muchas organizaciones existentes. (Carrel - Billiard et al., 2022)

9. Ciberseguridad

9.1 GDPR y ciberseguridad

Según una encuesta realizada en 11 sectores a los CEO's de las empresas más influyentes del mundo, concluyeron que la ciberseguridad va a ser el mayor riesgo para las empresas en los próximos tres años. No es de extrañar, ya que la cifra en 2021 de organizaciones afectadas por ataques de ciberseguridad era del 57%. Uno de los principales problemas que causan esto es la falta estimada de 2,72 millones de trabajadores cualificados y formados en ciberseguridad. A medida que estos ciberataques se multiplican, es probable que los equipos sin personal ni cualificación se enfrenten a altos niveles de estrés que afectarán a la capacidad de reaccionar y responder correctamente a estas amenazas. (Samartsev & Perucica, 2022)



Las empresas y organizaciones están teniendo muy en cuenta el aumento de los ataques de ciberseguridad. En una encuesta realizada, el 87% de los ejecutivos tienen planes para mejorar la ciberresistencia y reforzar sus políticas, procesos y normas de resiliencia para el futuro compromiso con terceros y la forma de gestionarlos. Hoy en día, la ciberseguridad debe considerarse una prioridad empresarial, especialmente con el aumento de los ataques y los que están por venir. El 84% de las personas que respondieron a una encuesta sobre "Obtención de liderazgo para la ciberseguridad" creen que la ciberresiliencia en su organización con la dirección y el apoyo de la dirección, pero el 68% cree que esta cuestión forma parte de su gestión de riesgos general. Se trata de una brecha bastante grande y los líderes de seguridad han planteado el problema de que, debido a ello, no participan en las decisiones de la empresa, lo que lleva a que se produzcan problemas de seguridad y se tomen decisiones menos seguras. La encuesta reveló que el 59% de los encuestados afirmó que les resultaría difícil responder a un ciberataque debido a la escasez de conocimientos necesarios en su equipo.

Las pequeñas y medianas empresas (PYMES) se sitúan como una amenaza clave para las cadenas de suministro, las redes de socios y los ecosistemas. El 88% de los encuestados ha declarado estar preocupado por las PYMES en su ecosistema. (Jurgens, 2022)

En base a estos resultados de la encuesta, está claro que la ciberseguridad debe ser más prioritaria en las organizaciones y ser "...vista como una cuestión estratégica de negocio que impacta en la toma de decisiones."

"La Inteligencia Artificial podría mejorar la ciberseguridad identificando comportamientos sospechosos, prediciendo ciberataques y manteniendo los datos seguros". (Jurgens, 2022)

Estas violaciones tienen un coste elevado que asciende a una media de 3,6 millones de dólares por incidente una caída media del 3% en la cotización de las acciones en 6 meses y, además, una empresa tarda una media de 280 días en identificar y responder a estos ataques. Para 2025, se espera que los costes de estas violaciones se disparen hasta los 10,5 billones de dólares. El coste financiero de los ciberataques a las empresas ha aumentado un 150% desde 2018. Esto crea enormes riesgos para las empresas y se traduce en resultados financieros y precios de las acciones negativos. (Jurgens, 2022). (World Economic Forum, 2022).

Hubo un aumento significativo de los ciberataques durante la pandemia debido a la mayor cantidad de trabajadores que trabajan a distancia. Sólo el 6% de los trabajadores realizaban trabajos a distancia antes de la COVID-19, que aumentó al 35% en mayo de 2020. En este plazo, las primeras 6 semanas de aumento del trabajo a distancia, se produjo un aumento de cinco veces en los ataques a estos trabajadores a distancia, pasando del 12% al 60%. Se realizó una encuesta en la que el 51% de los encuestados declaró que tras el cambio a un modelo de trabajo remoto se produjo un aumento del phishing en el correo electrónico. Esto ha llevado a que el 79% de las empresas experimenten un mayor tiempo de inactividad que conlleva una menor productividad debido a los ataques en ciberseguridad durante las temporadas altas. (Bechtel y Buchholz, 2022). (Dolezal, 2021)

Desde la pandemia, el trabajo a distancia se ha convertido en algo mucho más común que proporciona más oportunidades a estos ciberdelincuentes. Los trabajadores a distancia, por ejemplo, son más fáciles de atacar fuera de los cortafuegos corporativos y de las pasarelas de seguridad web. Dependen de las redes domésticas y de las conexiones VPN para acceder a aplicaciones y datos basados en la nube, y con frecuencia utilizan dispositivos desprotegidos. Además, los equipos de seguridad tradicionales en las instalaciones suelen

estar construidos para manejar redes de nivel empresarial y no para el acceso a Internet en el hogar. (Bechtel y Buchholz, 2022).

A las empresas les preocupa que, debido al aumento del trabajo a distancia, sea más difícil detectar la diferencia en la actividad de los usuarios con respecto a los comportamientos anormales cuando los empleados inician sesión desde diferentes lugares, lo que puede dar lugar a falsos positivos. Es un reto supervisar y gestionar todos los dispositivos remotos y su comportamiento, especialmente cuando son gestionados por orquestadores. (Bechtel y Buchholz, 2022).

9.2 Cómo reducir el riesgo de ciberataques

Existen algunas soluciones para reducir estos ciberataques, como la inteligencia artificial. "La Inteligencia Artificial podría mejorar la ciberseguridad identificando comportamientos sospechosos, prediciendo ciberataques y manteniendo los datos seguros". (Jurgens, 2022)
La Inteligencia Artificial puede ayudar de muchas maneras, una de ellas es que puede ayudar a los equipos de seguridad con pocos recursos. La IA puede utilizarse para reforzar los procesos de gobernanza de datos de las organizaciones. Algunos ejemplos de lo que la IA puede hacer en términos de reducción de tales violaciones es que puede tamizar a través de una multitud de fuentes con el fin de identificar los datos sensibles. A continuación, la organización puede "analizar, eliminar, cifrar o proteger de otras maneras de las amenazas externas o internas". Este uso de los datos permite a las empresas manejar la información confidencial de forma segura y también cumplir con las regulaciones y normas de privacidad como el GDPR. Además, la IA es capaz de crear datos sintéticos que a su vez crean escenarios y pronostican la posibilidad de una futura ciber exposición. De hecho, se dice que las organizaciones que han adoptado la IA y la automatización han experimentado costes de violación de datos mucho menores que las que no la han adoptado. (Samartsev & Perucica, 2022)
Otras soluciones utilizadas son la formación de los empleados en ciberseguridad, las copias de seguridad offline y los ciberseguros. También se ha aconsejado que las organizaciones busquen una solución de ciberseguridad basada en una plataforma que pueda detener los ataques de ransomware conocidos en todos los vectores de ataque. Esto requiere una estrategia de seguridad por niveles que combine controles proactivos de la red, de los puntos finales y del centro de datos basados en la inteligencia sobre amenazas globales. (Jurgens, 2022).

Según una encuesta realizada por el “World Economic Forum”, su conclusión fue que las empresas deben cambiar su enfoque de la ciberseguridad a la ciberresiliencia. La resiliencia cibernética es la capacidad de "resistir y recuperarse de los peligros y amenazas". Esto significa que las empresas que cuentan con estrategias estarán preparadas para los ataques antes de que lleguen y estarán mejor equipadas para hacer frente a los daños digitales. Una forma de hacerlo es mantener una copia de seguridad en formato no digital en caso de que los dispositivos digitales se caigan. Un ejemplo sería tomar nota de todos los números de teléfono necesarios a lo largo de una jornada laboral media. También involucrar a los ciberlíderes en las decisiones y discusiones de la empresa puede prevenir la gravedad de los ataques. En resumen, el plan y la práctica puestos en marcha por la empresa pueden reducir el daño causado por un futuro ataque. (*How We Can Protect Ourselves From Cybersecurity Threats In 2022*, 2022)

10. Análisis de la investigación

10.1 Impacto de la pandemia en el trabajo

De las seis personas que entrevisté, cuatro de ellas tenían sistemas establecidos para trabajar a distancia antes de que llegara la pandemia. De hecho, el 25% de la empresa del entrevistado B trabajaba a distancia antes de la pandemia y alrededor de una cuarta parte de su empresa ya había adoptado un enfoque híbrido antes de COVID-19 en el que trabajaban de forma programada uno o dos días a la semana o dos días al mes en la oficina. Del mismo modo, el entrevistado D trabajaba a distancia un día a la semana antes de la COVID, pero admite que él era una excepción dentro de su empresa, ya que el 95% del resto del personal trabajaba a tiempo completo en las instalaciones. Antes de COVID, tenía flexibilidad para elegir el día en el que podía realizar el trabajo a distancia y solía elegir un día en el que no tenía que asistir a ninguna reunión y en el que tenía que realizar un trabajo independiente que podía llevar a cabo desde casa.

Curiosamente, el director general de la empresa del entrevistado F, que es un líder tecnológico mundial, intentaba demostrar que el trabajo a distancia es eficaz antes de que se produjera la pandemia. Llevó a cabo un experimento en el que iba a trabajar desde África para demostrar que no necesitaba estar en la oficina para ser un director general de éxito y para demostrar que el trabajo puede llevarse a cabo con la misma eficacia desde fuera de la oficina. Así que cuando la pandemia llegó, concedió a todo el mundo permiso para trabajar a distancia a las dos semanas del comienzo de la pandemia. El entrevistado cita a su jefe diciendo "...todo el mundo puede trabajar a distancia para siempre". A las dos semanas de la pandemia, el director general de esta empresa había decidido que ese era el futuro.

El entrevistado F no trabajaba a distancia semanalmente, ni mensualmente, sin embargo, su empresa tenía una jornada intensiva antes de la COVID que les permitía trabajar desde casa un día al mes durante el verano. Sin embargo, dice que su empresa estaba muy en contra de trabajar desde casa antes de la pandemia, al igual que el entrevistado C. El entrevistado A estaba al 100% en la oficina antes de la pandemia.

La transición del trabajo en la oficina al trabajo a distancia habría afectado más a los entrevistados A y C, ya que no tenían ninguna opción de trabajo a distancia antes de la pandemia. Hablé con la entrevistada A sobre las barreras que se encontraron al pasar del trabajo de oficina al trabajo a distancia en su empresa. Dijo que el trabajo realizado por el departamento de TI y los equipos de salud y seguridad de su empresa aumentó. También habló de las barreras personales que tenían los empleados, como que al principio no querían encender sus cámaras porque no se sentían lo suficientemente respetables al no llevar su ropa habitual de oficina o no se sentían cómodos mostrando su origen en casa a sus compañeros de trabajo. Para superar esta barrera, se les dio diferentes fondos que mostraban diferentes oficinas de todo el mundo. Así, tanto si el empleado trabajaba desde la mesa de su cocina como desde su dormitorio, podía ponerse un telón de fondo para sentirse como si estuviera en un entorno de oficina durante las reuniones de equipo.

El entrevistado C dijo que su empresa tenía el mismo problema y que los empleados consideraban que las videoconferencias eran demasiado intrusivas para algunos miembros de su equipo, por lo que cambiaron a las llamadas de audio, que, según él, siguen siendo igual de eficaces. Se trata de dos soluciones diferentes para superar las barreras a las que se enfrentaban estas empresas al principio de la pandemia.

La otra barrera a la que se enfrentaron los empleados de las empresas que entrevisté fue el software de conferencias web que empezaron a utilizar al principio del cambio al trabajo de oficina a tiempo completo. Tanto el entrevistado D como el E empezaron a utilizar el software "Cisco Web Ex" para sus llamadas de vídeo y conferencias, y ambos afirmaron que era de mala calidad e improductivo. De hecho, ambas empresas, con sede en distintos países, se pasaron a "MS Teams", que, según dijeron, facilitó mucho la transición.
El entrevistado también habla de que su trabajo es más adecuado para ser realizado en la vida real debido a la naturaleza de su trabajo. Es un responsable regional de cumplimiento de la ética en el que tiene que llevar a cabo investigaciones de acoso, así como otras investigaciones, que le resultaban más difíciles mediante el uso de video llamadas. Dijo que juzgaba completamente mal a las personas a través de las reuniones por vídeo, ya que cree que no pueden comunicarse tan bien, a veces debido a las barreras lingüísticas, pero también por su lenguaje corporal. Dijo que juzgaba mal a la gente por no ver su lenguaje corporal, algo que las reuniones en línea borraron para él.
El entrevistado B no tuvo que enfrentarse a casi ninguna barrera durante este tiempo sin precedentes, ya que habían pasado por un programa de cambio a finales de 2014 en el que se eliminaron todos los ordenadores de sobremesa de la empresa y todos recibieron un portátil que les permitía el acceso remoto. Dieron a sus trabajadores identificaciones de acceso remoto y tokens de identificación seguros, de modo que esto les permitió trabajar desde casa antes de la pandemia si alguna vez lo necesitaban. Diseñaron este programa de cambio como parte de un plan de recuperación de desastres en la continuidad del negocio, de modo que, si alguna vez había un problema con la infraestructura, los centros de datos o el edificio, la gente podía continuar su jornada de trabajo a distancia. Antes de la pandemia, todos los miembros del personal tenían que conectarse a distancia al menos una vez al mes para asegurarse de que este sistema funcionaba. Estas medidas tenían a esta empresa muy bien equipada antes de que el trabajo a distancia se convirtiera en una norma y el entrevistado B dice que "estábamos preparados para cuando llegara la pandemia", lo que significa que no perdieron tiempo en la transición que estaba ocurriendo en otras empresas en ese momento.

Pregunté a cada uno de los entrevistados si sentían que había un cambio en la productividad dentro de su organización durante la pandemia. El entrevistado B dijo que era demasiado difícil de medir en la línea de su trabajador, ya que trabaja en la parte de desarrollo de software, consultoría e ingeniería de la empresa. Además, como ya estaban al día con las

últimas tecnologías y tenían sistemas establecidos para el trabajo a distancia, dijo que era difícil medir si había incluso un descenso de la productividad o un aumento. Sin embargo, dice que muchas de las personas que trabajaban en operaciones y ventas en su empresa tenían mejores registros para medir su productividad a través del número de llamadas que hacían, sus tiempos de respuesta y los tickets. Sin embargo, el resto de los entrevistados consideran que sí hubo un aumento de la productividad en sus empresas en esta época. El entrevistado D cree que el aumento de la productividad en su empresa se debió al cierre y al hecho de que las actividades sociales estaban cerradas, por lo que había más tiempo para trabajar. Sin embargo, aparte de esto, tomaron medidas para estabilizar su productividad creando un programa de recompensa y reconocimiento para reconocer el duro trabajo de sus empleados en este difícil momento de cambio. También se ofrecieron recursos a sus empleados para que pudieran realizar un trabajo adecuado desde casa.

La entrevistada A admite que al principio de este periodo de cambio hubo un bajón inicial, pero en general cree que el cambio al trabajo a distancia aumentó la productividad. Habló de algunos factores que su empresa debió tener en cuenta cuando la oficina volvió a abrirse y de cómo estos factores aumentaron la productividad y el trabajo mientras ella lo realizaba en casa. Cree que era y es más productiva cuando lleva a cabo el trabajo desde casa, ya que tiene un trayecto de 1 hora de ida y vuelta a su oficina. Dice que, si alguna vez vuelve a la oficina a tiempo completo, habrá perdido inmediatamente 10 horas como mínimo de su jornada laboral. Aunque trabaja desde casa, se levanta a la misma hora, pero puede empezar a trabajar una hora antes, y cree que su empresa ha recibido 10 horas más de trabajo de ella, y otras semanales, debido a la situación de trabajo a distancia. La entrevistada C también tenía las mismas preocupaciones a la hora de volver a la oficina. Dijo que antes de la pandemia su organización no fomentaba el trabajo a distancia, pero que se sorprendió cuando se puso en marcha durante la pandemia de que les funcionara tan bien. Dijo que muchos de los miembros de su oficina se trasladaron a otros lugares de Irlanda porque los precios de los alquileres aumentaron en Dublín, lo que significa que, si la oficina se abriera a tiempo completo, todos tendrían que desplazarse durante más de una hora. El entrevistado C tenía una hora de viaje a la oficina mientras trabajaba allí a tiempo completo y también cree que quitarle ese tiempo al día le hace más productivo en el trabajo. Incluso dice que su empresa debe tener en cuenta el largo viaje que tienen que hacer sus empleados para ir a la oficina, si es que tienen que volver, ya que la gente "simplemente se irá", ya que el trabajo a distancia es la norma en la mayoría de las empresas hoy en día.

El entrevistado D también habla de cómo se ahorró dos horas al día al no tener que desplazarse al trabajo, lo que también supuso un aumento de la productividad. También menciona algunas de las dificultades que pueden haber causado un descenso en su productividad al principio de la pandemia. Como sus hijos no iban a la escuela y tenían que ser educados en casa, le resultó muy difícil equilibrar su trabajo y su vida personal en ese momento. Admite que, si no hubiera tenido la ayuda de su pareja en ese momento, no habría podido hacer ambas cosas. Una forma de solucionar este problema era empezar a trabajar antes, dos horas antes de que se levantaran sus hijos, para que cuando le distrajeran durante el día no fuera tan importante. La entrevistada A también habló de cómo trabajar desde casa mientras sus hijos tenían que ser educados en casa causó una caída en la productividad al principio de la pandemia para su empresa también hasta que la gente encontró su rutina que podía equilibrar ambas cosas, similar a la entrevistada D.

Como ya no hay cierres en ninguno de los países en los que trabajan los entrevistados, pensé que sería interesante averiguar si volvían a su oficina a tiempo completo, seguían trabajando desde casa o adoptaban un enfoque híbrido. Curiosamente, todos ellos, excepto el entrevistado C, han adoptado un enfoque híbrido para trabajar después de la pandemia. El entrevistado C, en cambio, realiza todo su trabajo a distancia desde el comienzo de la pandemia. Esto es sorprendente, ya que su empresa no apoyaba en absoluto el trabajo a distancia antes de la pandemia. Me dijo que, como trabaja en TI, su trabajo es muy independiente, lo que significa que no necesita ir a la oficina para reuniones o proyectos de trabajo en equipo en los que los entrevistados tienen que participar.

Los entrevistados B, D, E y F adoptan un enfoque híbrido en el que trabajan desde casa uno o dos días a la semana. Todos estos entrevistados tienen que viajar como parte de su trabajo, por lo que pueden seguir viajando después de la pandemia y el uso de conferencias web que se utilizaba para sustituir esto, ha disminuido en los últimos meses.

La entrevistada A también realiza dos de sus cinco días en la oficina, mientras que el resto lo pasa trabajando desde casa. Dice que es necesario, ya que algunos de los proyectos que tiene que llevar a cabo son más eficientes si se hacen en persona. Pregunté a la entrevistada A que, si tuviera que volver a la oficina a tiempo completo, los empleados de la organización responderían positiva o negativamente. Me sorprendió escuchar que el 60% de sus compañeros de trabajo preferirían volver a la oficina a tiempo completo. Sin embargo, su situación ideal sería volver a la oficina, pero con un horario flexible, algo que los cambios tecnológicos que se produjeron durante el COVID permiten. Me puso el ejemplo de que, si

uno de sus hijos estuviera enfermo antes de la pandemia, tendría que tomarse el día libre para llevarlo al médico. Mientras que ahora, si su hijo estuviera enfermo, podría llevarlo al médico y seguir trabajando desde casa ese día o ir a la oficina por la tarde, por lo que su empresa no está perdiendo un día completo de trabajo. También dijo que la razón por la que la mayoría de la gente está a favor de trabajar en la oficina es por las interacciones sociales que se derivan de ello y también porque su casa puede volver a ser sólo su casa, mientras que durante la pandemia era su oficina de trabajo y su casa. La distinción hace que sea más fácil relajarse mientras se está en casa en lugar de tener acceso constante a su trabajo por las tardes.

10.1.1 Impacto de la tecnología en el trabajo

En esta sección he preguntado a los entrevistados cómo ha cambiado la naturaleza de su trabajo debido a los avances tecnológicos y cómo esperan que su trabajo evolucione y cambie en el futuro.

La entrevistada A trabaja en la selección de personal y dice que la naturaleza de su trabajo ha cambiado significativamente debido a los cambios tecnológicos. Cuando empezó a trabajar en este puesto hace quince años, los candidatos tenían que enviarle un currículum que presentaban a través de un portal web y luego el candidato esperaba la respuesta para ver si podía conseguir una entrevista para esta empresa en las semanas siguientes. Ahora, alguien presenta su solicitud en línea y recibe un correo electrónico automático de vuelta, en su lengua materna, de que la empresa ha recibido su solicitud. Además, la inteligencia artificial del sistema que tienen clasificará a los candidatos en función de quiénes son los más adecuados para el puesto que han publicado. Esto ha agilizado mucho su trabajo y revisará los cuatro mejores candidatos y se pondrá en contacto con ellos a través del correo electrónico en su sistema. También podrán recibir actualizaciones en directo sobre la fase del proceso de solicitud en la que se encuentran y si hay algún problema.

Tanto ella como otros gestores tienen plena visibilidad de los perfiles de los candidatos y pueden acceder a los datos mucho más rápido que antes gracias a la IA del sistema. Dice que "lo que habría llevado un par de semanas -.... ahora lleva de 24 a 48 horas". Dice que este aumento de la tecnología ha creado una expectativa para ella misma y para los candidatos de que ese es el plazo más corto. Mencionó que el trabajo que empezó a hacer cuando se incorporó a la empresa hace cinco años lo hacen ahora otras personas, pero que

éstas disponen de mucha más tecnología y herramientas que las que ella tenía cuando realizaba el trabajo. Esto se debe a la nueva tecnología en la que invirtió su empresa el pasado mes de octubre. En su antiguo puesto tardaba diez minutos en realizar un proceso que ahora sus compañeros tardan el doble.

También habla de la diferencia en las entrevistas, que antes se hacían cara a cara,

También habla de la diferencia en las entrevistas, que antes se hacían cara a cara, y que ahora se pueden hacer de forma eficiente a través de una reunión por vídeo.

También habla de cómo ha cambiado su industria en general. Trabaja en la industria farmacéutica, y antes la gente tenía que llamar a un médico y reservar una cita, mientras que ahora sólo tienen que rellenar un rápido formulario en línea sin llegar a reunirse físicamente con el médico.

Dice que los cambios tecnológicos han agilizado todos los procesos de su organización y han hecho que estos procesos, antes mundanos y largos, sean ahora muy fáciles de navegar. Además, los avances tecnológicos han aumentado las expectativas en su lugar de trabajo y afirma que incluso cuando alguien viaja en tren o en avión se espera que esté localizable y pueda trabajar.

Al igual que el entrevistado A, el entrevistado D habla de cómo los cambios tecnológicos han agilizado los procesos de su función. Afirma que la antigua forma de trabajar requería mucha mano de obra y presentaba un alto riesgo de errores humanos. La introducción de la automatización en su función ha aumentado la forma en que se realizan estos pasos y ahora dice que este trabajo que sólo realiza una persona no es óptimo para una empresa que quiere crecer rápidamente. Admite que se quedaría "sin trabajo" si no fuera por las nuevas tecnologías.

El entrevistado B también habla de cómo los cambios en la tecnología han modificado la naturaleza del trabajo de su organización. Cuando empezó en el mundo de la informática, hace veinticinco años, gestionaba centros de datos o salas de ordenadores in situ en las empresas. Ahora los ordenadores de sobremesa se han eliminado de su lugar de trabajo y ha visto un cambio masivo en la movilidad de los usuarios, ya sea que se conecten desde ordenadores portátiles, iPads, dispositivos móviles y ha visto una expansión masiva de las redes como las redes inalámbricas, las redes celulares y la conectividad. También menciona cómo las salas de ordenadores se han trasladado de las salas de ordenadores de las personas en las oficinas físicas a la nube o a los centros de datos. Esto ha cambiado en gran medida su forma de trabajar ahora y la naturaleza de todos los que trabajan en sus organizaciones.

El entrevistado C también habla de que el mayor cambio en la naturaleza de su trabajo es

que todo el mundo se ha trasladado a la nube. Explica que esta transición a la nube, como Google Cloud, ha supuesto una gran diferencia en su trabajo, ya que todos los miembros de la organización tienen copias de seguridad de sus datos en esta nube y ha transformado el funcionamiento de su empresa.
El entrevistado F trabaja en una plataforma global en línea y ha dicho que el aumento de la tecnología ha afectado mucho a su trabajo. Trabaja en el ámbito de la seguridad, por lo que antes sólo se ocupaba del acoso que se producía en persona, pero el aumento de la tecnología ha provocado un incremento del cibera coso. Dijo que el hecho de que la gente tenga acceso a esta plataforma en todo momento hace que sea extremadamente difícil, tanto para los niños como para los adultos, escapar del abuso. La tecnología ha mantenido estos comportamientos y ha añadido un reto adicional a la naturaleza de su trabajo.

A continuación, les pregunté sobre la introducción de robots en las industrias, la automatización y la creación de nuevos puestos de trabajo como consecuencia de ello. La entrevistada A dijo que, desde que entró en la empresa hace cinco años, su puesto de trabajo ha evolucionado cuatro veces y que el puesto que ocupa ahora no existía ocho meses antes. Este puesto se creó para ella y ahora es una función muy lógica en una organización, aunque ella fue la primera persona de la organización que ocupó este puesto. También se crearon otras funciones nuevas en su lugar de trabajo. Hace poco contrató a alguien para que fuera "On Site Engagement Manager", una función que se había creado para esta empresa. Esta función consiste en que alguien tiene que conectarse con el personal que trabaja fuera de TI desde una perspectiva de ciberseguridad y acceder a las necesidades únicas de este personal; como los riesgos particulares que podrían encontrar, para asegurar que el empleado está protegido mientras viaja y para asegurar que la empresa o el empleado no están en riesgo. Sin embargo, sólo se ha creado un papel realmente relevante.

El entrevistado F está de acuerdo en que se van a destinar mayores presupuestos a la creación de nuevos puestos de trabajo en informática y ciberseguridad por encima de la seguridad física en las diferentes organizaciones.

El entrevistado C ha mencionado cómo su papel como propietario de producto sólo va a evolucionar debido a los cambios tecnológicos, pero ya ha visto cómo la automatización está asumiendo nuevos puestos de trabajo y creando otros nuevos. Utiliza el ejemplo de que Google ha creado una función completamente nueva en los SRE y su trabajo consiste en

mantener la infraestructura en funcionamiento. También cree que los nuevos puestos de trabajo, como los SRE y los propietarios de productos, serán más comunes que los desarrolladores, los analistas, los gestores de proyectos y los gestores de programas, que tienen más probabilidades de ser automatizados. En los centros de llamadas de su empresa, ya ha visto cómo se produce la automatización. Las personas de su centro que se ponen en contacto con los clientes para confirmar los ingresos, los gastos y los activos se apoyan ahora en la tecnología y el plan de la empresa a corto plazo es sustituir a las personas que trabajan en estas funciones por máquinas automatizadas.

El entrevistado D está realmente implicado en la introducción de la automatización y las tecnologías en la fabricación. "Creo que todavía hay que hacer grandes avances con la automatización, los robots colaborativos, la inteligencia artificial, la realidad aumentada y el análisis de datos". Su papel es estar en contacto con los avances tecnológicos y llevarlos a su empresa. Cree que su papel como director de fabricación evolucionará siendo proactivo y realizando mejoras en la eficiencia de la fabricación a través de la analítica de datos.

La entrevistada A también me contó cómo el uso de robots ayudó enormemente a su empresa en su anterior trabajo en otra compañía. Su anterior empresa se especializaba en coches y en la fabricación de diferentes piezas para los mismos, especialmente para los Tesla. Para ello, tenían un robot de ocho ejes en sus instalaciones de Estados Unidos y este robot se utilizaba para cortar y trocear piezas para los coches. El entrevistado cuenta que la precisión y la velocidad con la que trabajaba el robot, ningún humano podría competir con él. Dijo que sin el uso de este robot, la fábrica, que contaba con 200 empleados, no podría seguir en el negocio y mantener los niveles de productividad altos. Como Tesla estaba sacando un nuevo coche, necesitaban una gran velocidad en sus procesos para poder cumplir con ciertos plazos que se les habían dado. Sin embargo, está de acuerdo en que la introducción de robots en el lugar de trabajo aumenta la productividad en la fábrica y crea más trabajo y funciones para otros empleados. Sin el robot haciendo su trabajo, el resto del trabajo en los coches no podría haberse realizado. Afirma que tiene que haber una asociación entre robots y humanos en el lugar de trabajo, y que la automatización no sustituye a las personas, sino que, de hecho, "...crea más oportunidades profesionales".

El entrevistado B tiene una postura similar sobre cómo los robots van a sustituir los puestos de trabajo. Cuenta que el mismo argumento se utilizó en 1959, cuando se utilizaron máquinas para cosas como las tarjetas perforadas, que pueden ser realizadas por máquinas en lugar de por personas, lo que abrió todo un nuevo mundo de la informática y la tecnología de los ordenadores. "En realidad no quitó puestos de trabajo, sino que cambió por completo la forma de trabajar y cambió por completo las empresas y el mundo del trabajo. Así que en lugar de quitar los puestos de trabajo de millones y millones de puestos de trabajo en los últimos 40 o 50 años, es exactamente lo mismo en la próxima evolución de la tecnología".

También dice que la automatización y los humanos tienen que aprender a trabajar juntos para tener éxito. Cree que la automatización va a desempeñar un papel importante en una empresa cuando sustituya a las personas para llevar a cabo tareas mundanas y repetitivas, que suelen estar orientadas a los procesos y que es mejor que las realice una máquina. Explica las tareas que están desempeñando un papel en la automatización de procesos robóticos (RPA), en la que se enseña a un ordenador a realizar un tipo concreto de macro tarea y todos los criterios que cumplen este tipo de tarea, el ordenador y las máquinas son capaces de realizarla. Del mismo modo, habla de cómo la automatización es útil en las pruebas de software y se utiliza en el trabajo de ciberseguridad. Una máquina automatizada puede detectar amenazas vulnerables y probar esas amenazas en el sistema que un humano nunca sería capaz de probar al mismo ritmo. Sin embargo, la automatización y los robots sólo pueden llevar a cabo un proceso hasta un nivel determinado y entonces es cuando los humanos tienen que entrar y terminar el proceso. Los resultados de los informes que han sido probados por las máquinas automatizadas, en este ejemplo, tienen que ser revisados por un humano porque esta corrección podría ser completamente diferente para diferentes sistemas. Los robots nunca podrán conocer el contexto que hay detrás de un código de software que se ha desarrollado de una manera determinada y ahí es donde un humano tiene que terminar el trabajo y arreglar la vulnerabilidad detectada por la máquina, según el entrevistado. Básicamente, cree que en la gestión de las ciber infraestructuras, la ingeniería y el uso de los centros de datos es donde la inteligencia artificial y la automatización tienen un papel vital que desempeñar. El uso de estas tecnologías podrá analizar rápidamente los datos basados en el historial y predecir si va a haber un fallo. Por ejemplo, pueden utilizar estas tecnologías para analizar 3.000 tickets que se introdujeron en el sistema durante cuatro años. Pueden clasificar los tickets y predecir que el sistema va a fallar si despiden a un determinado gestor de eventos o si realizan un nuevo cambio en la organización que causará

problemas. La inteligencia artificial y la automatización pueden clasificar las cosas importantes que deben tener en cuenta los gestores, algo que no podría hacer eficazmente un humano.

También cuenta que algunas empresas están cometiendo errores a la hora de implantar la automatización en la plantilla. Dice que no tiene sentido automatizar tareas que requieren inteligencia o comportamiento humano, va a ser costoso y poco exitoso, según su experiencia. El equilibrio más exitoso es utilizar máquinas y humanos en las proporciones adecuadas y contratarlos en los trabajos en los que son más adecuados.

El entrevistado E cree que la tecnología y la automatización se harán cargo del sector jurídico hasta cierto punto, pero en su función de invertir en el acoso, no ve que los robots o la automatización puedan realizar este trabajo en un futuro próximo. Necesita evaluar la situación desde diferentes ángulos y tener el conocimiento para saber que hay dos lados en cada caso que tiene que tratar, algo que los robots no podrán hacer en los próximos 15 o 20 años, en su opinión.

Todos los entrevistados creen que en el futuro habrá que mejorar las cualificaciones y reciclarlas para adecuarlas a los nuevos puestos de trabajo que se crearán, sobre todo porque el sector que más puestos de trabajo va a crear es el de las tecnologías de la información. La entrevistada A cree que la actualización de las competencias es esencial, ya que si los empleados se quedan con el papel que tienen actualmente sin formación adicional, se quedarán sin trabajo en el futuro. La entrevistada A me cuenta que ha ido a la universidad tres veces a lo largo de su vida, y no es algo inusual en su organización. En su empresa se anima a los trabajadores a realizar constantemente cursos a tiempo parcial fuera del trabajo para estar a la vanguardia y mantener una ventaja competitiva. Los entrevistados C y D están de acuerdo en que será necesaria una sólida formación para mantenerse a la vanguardia y poder adaptarse a las nuevas funciones que se creen en el futuro.

El entrevistado B profundiza en lo que cree que la gente tendrá que hacer para mantenerse en línea con el futuro. Cree que la gente tendrá que actualizar sus conocimientos, reciclarse y formarse de forma cruzada. Sin embargo, hay una generación que viene de un mundo digitalmente nativo, que ha nacido en la tecnología y que tiene un alto conocimiento de cómo funciona la tecnología en el momento en que entra en la fuerza de trabajo. Cree que

han nacido en el mundo digital y pueden convertirse fácilmente en tecnólogos porque tienen un nivel de conocimientos básico diferente al de los demás.

10.1.2 Impacto GDPR

Para esta sección pregunté a mis entrevistados qué medidas habían puesto en marcha sus empresas para garantizar que no se produjeran violaciones de datos al pasar al trabajo a distancia, hablamos de los ciberataques y del riesgo que supone para las empresas en el mundo laboral moderno.

El entrevistado C habló de cómo su empresa sufrió una violación masiva de datos hace cuatro años, antes de la pandemia. Cómo ocurrió es que se detectó una vulnerabilidad en el sistema y eso hizo que los hackers pudieran acceder a su sistema y robaron los datos personales de 150 millones de personas en Estados Unidos que eran clientes de esta empresa. Explica que fue un caso muy sonado en el que tuvieron que intervenir los gobiernos. A partir de esta brecha, su empresa tuvo que pasar por un proceso de transformación y fue cuando su empresa trasladó todos sus datos a la nube. El aumento de la seguridad y la protección de los datos fue algo que esta empresa se dio cuenta de que tenía que aumentar la concienciación para garantizar que algo así no pudiera volver a ocurrir en el futuro.

El entrevistado B entra en detalles sobre cómo se producen los ciberataques y se debe a una infraestructura débil, a la escasa formación de los empleados y al entorno que permite la entrada de un hacker con el tiempo. Para explicar la debilidad de la infraestructura, me habló de los muchos elementos de la ciberseguridad, "desde lo básico de la protección antivirus en todos tus dispositivos, la seguridad de tus puntos finales, tus dispositivos móviles, además de tus servidores y la gestión de la detección de intrusiones". Explica que la detección de intrusos son los aparatos reales en el borde de la red que pueden detectar y aprender las intrusiones y pueden descargar información que se actualiza de los proveedores comerciales para decir que estos son los últimos eventos. La siguiente parte de la infraestructura es el programa de monitorización de malware, que supervisa el malware que "está en la naturaleza" en comparación con los cambios de archivos que se han visto en el sistema. A continuación, una empresa necesita mirar sus dispositivos vulnerables que contienen un "superusuario" o un "acceso de administración del sistema". Explicó que un atacante común atacará un punto de partida. Los integradores de sistemas, las empresas de soporte y las grandes consultoras suelen instalar dispositivos en su entorno para utilizarlos como punto

de partida, con fines de soporte o para arreglar el punto vulnerable que parezca. Los puntos de salto suelen ser un punto vulnerable para una empresa, ya que suelen estar mal mantenidos, aunque el punto de salto tenga el acceso de superusuario al trabajo que hay que hacer, así que cuando un hacker entra en uno de ellos, es una gran amenaza para la empresa. Una parte de la infraestructura que se pasa por alto y que causa el mayor daño cuando se encuentra en un punto vulnerable ya que permite a los hackers entrar en el sistema. La siguiente cosa que es súper importante dentro de la infraestructura es el monitoreo de la exfiltración de datos. Por lo general, los hackers entran en el sistema pero no causan daños de inmediato. La supervisión de la exfiltración de datos tiene que ver con la gestión de datos y la detección de cambios en el sistema. Utilizó el ejemplo de un servidor, como el de Oracle, que normalmente transmite de 3 a 5 gigabytes entre los usuarios en Internet o los usuarios y el acceso remoto, y de repente empieza a transmitir 40 gigabytes al día. Esta debería ser la principal señal para que un sistema sea investigado de inmediato. La razón de este aumento de los datos que se están exfiltrando en un periodo de tiempo tan corto podría deberse a que alguien ha tomado los datos o los ha enviado a otro servidor. Así que aquí es donde una buena educación de los usuarios, la formación en ingeniería de ciberseguridad para los analistas de ciberseguridad y los directores de ciberseguridad es esencial para que sean capaces de detectar si algo es diferente para poder investigar.

Después de entender cómo se producen los ciberataques desde el punto de vista de las TI, pregunté a los otros entrevistados, que no pertenecen al sector de las TI, qué medidas se pusieron en marcha durante el cierre para asegurarse de que no sufrieran ninguna violación de datos durante este periodo de transición. La entrevistada A explicó que cuando se conecta de forma remota, su dispositivo móvil es su autenticación, ya que se le reconoce de forma exclusiva. Tiene una serie de números de pin para acceder a su portátil de trabajo y también tiene que utilizar su huella dactilar para evitar las filtraciones de datos. Si se conecta a su portátil de trabajo, no puede entrar en ningún otro sitio web que no sea Google hasta que se someta a esta doble autenticación. El entrevistado F también me habló de la autenticación en dos pasos que realiza su empresa cuando trabaja fuera de la oficina para garantizar la ciberseguridad. Del mismo modo, tienen una contraseña extremadamente segura que tiene que pasar un nivel de pruebas y para la segunda parte utilizan una "YubiKey" que es una llave negra que se encaja en el lateral de sus portátiles y tiene una huella del pulgar en la que tienen que tocar para activar su servidor de trabajo. Por último, la empresa del entrevistado B también utiliza una autenticación multi- factor para que las personas puedan entrar en sus portátiles desde cualquier lugar. Al igual que el entrevistado A, cuando el

empleado se conecta, se le envía un pin a su teléfono, y a veces aleatorizan el pin para que le permita abrir una aplicación o bien le envían un texto. No dicen a sus empleados qué método utilizan, de modo que si alguien ha pirateado su aplicación o su teléfono, pueden detectarlo inmediatamente y redirigirlo. La autenticación en dos pasos es un estándar en estas empresas.

La empresa del entrevistado E creó una red privada virtual (VPN) para garantizar que pudieran trabajar a distancia y de forma segura. También se encriptaron todos sus portátiles para que cuando trabajen desde casa y su portátil esté bloqueado, lo cual es una norma cuando cualquier persona de la empresa deja su portátil desatendido, se reduzca el riesgo de que se produzcan violaciones de datos y de que alguien robe su propiedad intelectual.

La empresa del entrevistado B también lleva a cabo dos métodos diferentes según el sistema que se utilice para garantizar la seguridad de los datos mientras las personas trabajan a distancia. El primero es una plataforma llamada Zen Scaler, que está en la nube y supervisa la conectividad a Internet de las personas que se conectan a ella. Esta plataforma sólo permite a los empleados conectarse a sitios de confianza y bloquea todos los demás sitios. Al igual que el entrevistado E, tienen túneles VPN para aplicaciones corporativas privadas.

Todas las empresas para las que trabajan han puesto un gran énfasis en la educación de los empleados en relación con la resiliencia cibernética y para reducir los ciberataques. Todos reciben formación y, de hecho, el entrevistado B lleva a cabo la formación en su respectiva empresa.

La formación que se realiza es similar en todas las empresas, el entrevistado D dice que realizan una formación de concienciación que da a los empleados ejemplos específicos de errores que podrían llevar a violaciones importantes. Además, algo común en todas las empresas es que reciben informes de "phishing" si encuentran que un correo electrónico es sospechoso. El entrevistado F dijo que su empresa, al igual que el resto, envía estos correos electrónicos de “phishing” para asegurarse de que no están "dormidos" durante el trabajo. La empresa del entrevistado A envía estos correos electrónicos cada poca semana para asegurarse de que saben cómo reaccionar ante ellos. Estos correos electrónicos se diseñan para que parezcan de personas legítimas, como clientes o personas con las que trabajan, y es el equipo de ciberseguridad el que se asegura de que no abran el correo electrónico o accedan al sitio web. Los empleados de su empresa reciben mucha educación y formación en este ámbito. También está capacitada para saber si la gente que la llama mientras está en el trabajo es legítima. Me contó un ejemplo de una ocasión en la que recibió una llamada

telefónica y le pidieron su número de PPS, pero inmediatamente supo que su proceso no funcionaba así y pudo informar de la llamada inmediatamente al equipo de TI. Ha habido casos en los que su equipo de TI ha rastreado estas llamadas y se ha asegurado de que no vuelvan a llamar a la empresa.

El entrevistado C afirma que es muy importante "crear una cultura de conciencia cibernética" dentro de las empresas, lo que, por supuesto, comienza con la formación del personal. En su empresa utilizan una combinación de estrategias, como boletines informativos, aprendizaje electrónico, sesiones informativas para los nuevos empleados y manuales sobre lo que deben hacer y lo que no deben hacer.

La empresa del entrevistado B también tiene algunas estrategias diferentes en lo que respecta a la formación de los empleados. Tienen un programa de cumplimiento anual y periódico. Cada año, los empleados tienen que recibir formación sobre ciberseguridad y pasar un examen. Se trata de un requisito básico para el empleo. También tiene lugar una formación más regular, por ejemplo, recertifica el acceso de sus equipos bianualmente. Así que cada seis meses, todos los empleados que trabajan para él tienen sistemas que se le envían y él los revisa y decide si necesitan formación adicional o no. Además, reciben correos electrónicos de phishing, exactamente igual que los demás. Si alguien hace clic en el enlace del correo electrónico, tiene que volver y realizar otro curso de ciberseguridad. Los antecedentes de cómo funciona el informe de phishing en su empresa son: si alguien hace clic en el correo electrónico, el equipo de TI recibe una notificación, ya que hay un botón de phishing en el correo electrónico, y el correo electrónico se elimina de la bandeja de entrada del empleado. Revisan las cabeceras y los pies de página del correo electrónico, encuentran el origen de este y, posteriormente, bloquean cualquier correo electrónico futuro procedente de esta ubicación.

Por último, la empresa del entrevistado D también vuelve a certificar sus equipos para asegurarse de que no suponen un riesgo para la ciberseguridad, y su empresa está pasando actualmente por un programa de remediación en el que están probando todos sus equipos antiguos para asegurarse de que son seguros.

11. Conclusión

El análisis de este trabajo de investigación ha llevado a la conclusión de que la transición al trabajo a distancia y la eficacia del trabajo a distancia dependen de muchos aspectos

demográficos y de la naturaleza de la función del empleado. De mi revisión de la literatura, he aprendido que aquellos que trabajan predominantemente en puestos de trabajo tienden a haber adoptado el trabajo a distancia más rápidamente. Esto es cierto, ya que el entrevistado C es el único que sigue trabajando a distancia después de la pandemia, ya que dice que su trabajo requiere mucho trabajo independiente y que su trabajo es muy tecnológico. También hay que tener en cuenta diferentes factores, como si los hijos de un empleado también estaban en casa durante la pandemia, lo que hemos visto que al entrevistado E le resultó difícil al principio crear una rutina para equilibrar su vida laboral y las necesidades de los niños. En conclusión, la eficacia del trabajo a distancia varía en función de la vida personal y profesional de cada uno, por lo que el enfoque híbrido fue la solución más común para trabajar después de la pandemia. Permite que la gente vaya a la oficina, pero ofrece una mayor flexibilidad que la que había antes de la pandemia mundial.

A lo largo de todos los años que cada entrevistado estuvo en su puesto, hubo una similitud general en cuanto a que la tecnología ha hecho que su trabajo evolucione significativamente con el tiempo, y seguirá evolucionando debido a la tecnología. Por ejemplo, la función de la entrevistada A ni siquiera existía en su empresa hace un año. Esto permite concluir que la introducción de las nuevas tecnologías en un lugar de trabajo no va a quitar puestos de trabajo, sino que, de hecho, va a crear un sinfín de puestos de trabajo que ni siquiera existen todavía. De mi investigación secundaria y primaria se desprende que se están creando más funciones nuevas en el sector de las tecnologías de la información en comparación con otros sectores. Además, según mis investigaciones, es importante que las empresas adopten estas nuevas tecnologías. Es necesario que se acepte que los robots y la automatización de los puestos de trabajo están ocurriendo y seguirán ocurriendo. Como dice el entrevistado B, tenemos que aprender a trabajar con los robots y utilizar a los humanos para sus puntos fuertes y a los robots para los suyos y se producirá una productividad óptima en los lugares de trabajo.

Por último, es cierto que los ciberataques son uno de los mayores riesgos en las empresas, especialmente en los próximos tres años. De mi investigación secundaria aprendí que hubo un aumento de los ciberataques durante la pandemia debido al aumento de personas que trabajan a distancia. Las empresas para las que trabajan los entrevistados adoptaron muchas medidas para garantizar la seguridad durante este periodo, como el inicio de sesión con autenticación múltiple, las redes privadas virtuales (VPN) y el almacenamiento de datos en la nube. La principal conclusión que he encontrado en este apartado es que la educación de los empleados es la medida más importante que se debe llevar a cabo para prevenir los

ciberataques y poder hacer frente a un ciberataque rápidamente si se produce. Dentro de todos los empleados entrevistados, todos han realizado una formación intensiva y regular para ser conscientes de las señales de un hacker que entra en el sistema.

Como conclusión general, la tecnología ha sido la principal razón por la que el trabajo se ha podido llevar a cabo con normalidad en todo COVID-19. Está cambiando los puestos de trabajo y la implantación de la tecnología en las plantillas está creando puestos de trabajo a diario. Aunque tiene sus riesgos, también ha ofrecido más oportunidades al trabajador actual.

12. Bibliografía

Awada, Mohamad, et al. "Working from Home during the COVID-19 Pandemic: Impact on Office Worker Productivity and Work Experience." *Work*, vol. 69, no. 4, Jan. 2021, pp. 1171–89, https://doi.org/10.3233/WOR-210301.

Awada, Mohamad, and Issam Srour. "A Genetic Algorithm Based Framework to Model the Relationship between Building Renovation Decisions and Occupants' Satisfaction with Indoor Environmental Quality." *Building and Environment*, vol. 146, Dec. 2018, pp. 247–57, https://doi.org/10.1016/j.buildenv.2018.10.001.

Balkeran, Arianna. "Hustle Culture and the Implications for Our Workforce." *Student Theses and Dissertations*, June 2020, https://academicworks.cuny.edu/bb_etds/101.

Bechtel, M., Briggs, B. & Buchholz, S., 2020. *Tech Trends 2020 - Horizon next: a future look at the trends,* Dublin: Deloitte.

Bechtel, M. and Buchholz, S., 2022. *Tech Trends 2022*. [online] Www2.deloitte.com. Available at: <https://www2.deloitte.com/content/dam/insights/articles/US164706_Tech-trends-2022/DI_Tech-trends-2022.pdf> [Accessed 6 April 2022].

Carrel - Billiard, M., Daugherty, P., & Blitz, M. (2022). *Technology Vision 2022 - Meet me in the Metaverse* [Technology Report]. Acenture.

Coros, S., 2019. *Robots will soon be a necessity but they won't take all our jobs*. [online] World Economic Forum. Available at: <https://www.weforum.org/agenda/2019/01/flat-packed-robots-delivered-to-your-door-could-soon-be-a-reality> [Accessed 6 April 2022].

Dolezal, A. (2021, November 9). *Cyber Threats Have Increased 81% Since Global Pandemic*. https://www.businesswire.com/news/home/20211108005775/en/Cyber-Threats-Have-Increased-81-Since-Global-Pandemic

Enache, R. & Puscas, A., 2020. *Remote work in the new reality,* Amsterdam: KPMG.

Feyrer, James. "Aggregate Evidence on the Link between Age Structure and Productivity." *Population and Development Review*, vol. 34, 2008, pp. 78–99, https://www.jstor.org/stable/25434760.

Goetzel, Ron Z., et al. “Health, Absence, Disability, and Presenteeism Cost Estimates of Certain Physical and Mental Health Conditions Affecting U.S. Employers.” *Journal of Occupational and Environmental Medicine*, vol. 46, no. 4, Apr. 2004, pp. 398–412, https://doi.org/10.1097/01.jom.0000121151.40413.bd.

Gorlick, A., 2020. *The productivity pitfalls of working from home in the age of COVID-19 | Stanford News*. [online] StanfordNews.com. Available at: <https://news.stanford.edu/2020/03/30/productivity-pitfalls-working-home-age-covid-19/> [Accessed 23 March 2022].

Grant. (2019, March 16). *How Does Technology Affect the Work Environment Today?* [How Does Technology Affect the Work Environment Today?]. Small Business - Chron.Com. https://smallbusiness.chron.com/technology-affect-work-environment-today-27299.html

Guerra, C. (2021, May 7). *Remote working is here to stay, but only if you want to — Z1 Blog*. Remote Working Is Here to Stay, but Only If You Want To. https://z1.digital/blog/remote-working-is-here-to-stay-but-only-if-you-want-to

Heschong, Lisa, et al. “Windows and Offices: A Study of Office Worker Performance and the Indoor Environment.” *Research Gate*, Jan. 2003.

How We Can Protect Ourselves From Cybersecurity Threats In 2022. (2022, January 19). World Economic Forum. https://www.weforum.org/videos/how-we-can-protect-ourselves-from-cybersecurity-threats-in-2022/

Hunter, Emily M., et al. “Violating Work-Family Boundaries: Reactions to Interruptions at Work and Home.” *Journal of Management*, vol. 45, no. 3, 2019, pp. 1284–308, https://doi.org/10.1177/0149206317702221.

Irwin, L. (2021, August 19). *The cyber security risks of working from home - IT Governance blog*. IT Governance UK Blog. https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home

Jurgens, J. (2022). *Global Cybersecurity Outlook 2022 INSIGHT REPORT JANUARY 2022*. Cologny: World Economic Forum.

Kokemuller, N. (2019, July 29). *Why Is Technology Important in Business?* Bizfluent.

https://bizfluent.com/about-6320228-technology-important-business-.html

Lund, S. et al., 2021. *The Future of work after COVID-19*, London: McKinsey & Company.

Madgavkar, A., Lund, S., Manyika, J. & Smit, S., 2020. *hat’s next for remote work: An analysis of 2,000 tasks, 800 jobs, and nine countries*, London: McKinsey and Company

Radin, J., & Korba, C. (2020, November 13). *COVID-19 as catalyst*. Deloitte Insights. http://www2.deloitte.com/us/en/insights/industry/health-care/health-care-workforce-trends.html

Roosaar, Liis, et al. “Age-Related Productivity Decrease in High-Waged and Low-Waged Employees.” *International Journal of Manpower*, vol. 40, no. 6, Jan. 2019, pp. 1151–70, https://doi.org/10.1108/IJM-03-2018-0086.

Santana, M. and Cobo, M., 2020. *What is the future of work? A science mapping analysis*. [online] Sci2s.ugr.es. Available at: <https://sci2s.ugr.es/sites/default/files/ficherosPublicaciones/2781_SantanaM-emj-2020.pdf> [Accessed 23 March 2022].

Shaffer, Margaret A., et al. “Expanding the Boundaries of Work—Family Research: A Review and Agenda for Future Research.” *International Journal of Cross Cultural Management*, vol. 11, no. 2, 2011, pp. 221–68, https://doi.org/10.1177/1470595811398800.

Shemesh, R. (2022, April 15). *What Is Cyber Resilience?* https://www.datto.com/blog/what-is-cyber-resilience?utm_medium=opengraph&utm_source=225

Singh, Jagdip, et al. “Sales Profession and Professionals in the Age of Digitization and Artificial Intelligence Technologies: Concepts, Priorities, and Questions.” *Journal of Personal Selling & Sales Management*, vol. 39, no. 1, Jan. 2019, pp. 2–22, https://doi.org/10.1080/08853134.2018.1557525.

Webb, A. (2022). *Artificial Intelligence - 2022 Tech Trends Report* (15th Edition). Future Today Institute. https://futuretodayinstitute.com/mu_uploads/2022/03/FTI_Tech_Trends_2022_Book01.pdf

Willems, M. (2022, January 5). *Tech Special: The jobs, sectors and countries most at risk of automation and robotics in 2022*. https://www.cityam.com/exclusive-the-jobs-sectors-and-countries-most-at-risk-of-automation-and-robotics/

World Economic Forum. 2021. *Robots and your job: how automation is changing the workplace*. [online] Available at: <https://www.weforum.org/agenda/2021/06/study-this-is-how-robots-are-expected-to-impact-future-workplaces> [Accessed 6 March 2022].

13. Apendicé

Todos los nombres de los entrevistados se han omitido por razones éticas. Todos los entrevistados han firmado un formulario de consentimiento para llevar a cabo la entrevista que puede ser enviado a petición.

Entrevistada A

Okay, so can you give me a brief description of your current role in AbbVie?

Yes. So, within AbbVie, I run recruitment activities across the US and effect. So, my team are responsible for recruiting in eight different locations in Ireland, France, Belgium, Germany and Italy. So I have 12 sites that my team support. Their day to day, they're involved in bringing in new talent into the business and promoting the talent that are currently there.

Okay, very good. And has the nature of your job changed at all over time due to technological advances?

Yeah, significantly, for us it's really reading the marketplace, and getting to our candidates is what's usually important to us. So even I would say in the last two years, like irrelevant of COVID, because I think what we brought its own changes to how people worked and how they use technology in their home and remotely, and would like for us from a candidate experience perspective. Now, like when I started recruiting, probably about 15 years ago, people had a resume CV, they may have submitted through a web portal. And then they waited to hear back and they hope to hear back at some point in the next number of weeks for an interview. Today, somebody applies online, they get an automatic email back saying that, thanks so much in their own native language, irrelevant for country they're in and they will be processed, we will use the technology. So we've different types of platforms. So when I'm reviewing profiles, the AI in the system will actually rank the person based on what we've posted. So it will do part of my job for me saying like, these are the people that are your top candidates to try and speed up my time for response, we'll engage with candidate through email through the system, they'll be able to do live status updates on how their application is progressing and if there's any issues with it. And then for our managers, everything we do, we send it out to the system. So they have full visibility in relation to candidate profiles, and always get access to the data for quicker. And so what would have been a couple of weeks of a timeframe, now you're down to like 24 or 48 hours and that's the expectation. And then very practically, like when we're interviewing, again, everything

we used to be face to face, you know, you're ranging and welcome somebody into reception area. Now, your interview process could be through Microsoft teams could be through zoom, you might pre record like, you know, I can send you a list of questions, and you could pre record your interview and send it to me. So from a technology point of view, for us, it's just changed hugely like when we're doing medicals pre employment medicals. Now used to previously, everybody would have got to care to get a doctor's appointment. Now what happens is typically you would fill out an online form, the doctor will review it in their time, and then come back and they'll pass someone have never met them. So it's from a technology point of view, it's like ease of technology throughout the process, and how, from a candidate experience perspective, we can make that better. But then, like for my team, like now, during COVID, like we would have been in the office a lot before COVID. And that's important. And it still is important to have that connection. But typically now, we just launched a new policy globally, that if you have flexibility, we want flexibility in the workplace. So you can work from home, you can work remotely, whatever two days week, like, you know, I remember one of my bosses sent me if you've got a decent Starbucks beside you, you can work with that. Because once you have Wi Fi sure doesn't matter where you are in the world, you know, you can log on. And that's the thing that can we expect people know, when they're flying, like, you know, at one time you checked in, that was a, you lost, like, whatever, two to 10 hours working time, because you're in the air. We communicate all the time now, because expectation is you just pay for your Wi Fi. And it's still it's like being on the train, you know, so a lot of those things, I think like buses, etc. They're all now and when Wi Fi enabled, so you have continuously can work like your whole working life now has changed and I think in particular in the last decade, and in the last few years.

Okay, very good. And so you worked full time in the office before COVID. Did you?

Yeah.

Okay. So obviously technology aided moving from the office to online, as you said, were there any barriers to this at all at the beginning?

Not necessarily barriers, but I do think it accelerated from our IT support team what they had to do, because I'm actually for safety or health and safety teams as well because the two things that emerged very strongly. I think the two barriers predominantly before COVID Was that, okay, from a cybersecurity perspective , how can we guarantee security and our Are we sure that what protocols have to be put in place like, from from a home life point of view, then the second piece of that was where from a safety point of view, you're in an

office, you're ergonomically set up with your chair, your table, your display monitors. How do you manage that for somebody at home? Because they're still in the working environment. Now they are at a home. And what happens if somebody falls down stairs? Is it now their workplace? You know, so there's all of those elements that came into play that COVID really forced an acceleration in response. Now I will say, I think during COVID people accepted a bit more. I'm still in my home. And maybe I'm working from the kitchen table, or maybe I'm working from my bedroom. Like even that, like a couple of years ago, if you saw somebody log around and zoom. We've all have our own backdrops, too, so that you can't see somebody's bed, or you can see that they're in the kitchen table. And if their kids are playing in the playpin behind them. But that element is there to make it look like they're still in an office, like if i think of my background, like I have about 20 different shots from the offices around the globe, that I can choose to make it look like I'm still in the office Because those sorts of things that can that were put in to make it more comfortable for people. Initially, and think people in the beginning, were a little bit reluctant turning on the camera, because it took a while for people to settle into their new workplace. So like those people would have said, "Oh, well, I'm just I'm not ready right now to be camera ready." Well, you're in work you would be camera ready? You know. So I think it took a little while in the beginning the COVID as well, for people to go, Oh, God, actually, I'm still in work. So like, you start to see people like dressing in the same way as they would have in the office, like, you know, as lean as opposed to their home clothes.

Exactly. And in terms of putting in measures to ensure there were no data breaches and stuff from moving online, were there anything any strategies put in place?

So there was far more robust security. So when I connect remotely, my mobile device is my authentification. So that is recognized uniquely to me. And so I have a series of pin numbers or protection numbers. And also, then I have to use my thumbprint to curb data breaches. When I try to log onto my laptop, I cannot enter any other site than Google unless I put all the authentication protocols in place. It takes two minutes to do it. So the speed of doing it has really improved. But it just means that for somebody to hack me, they have to have my laptop, they'd have to have my phone, and they'd have to have me like they couldn't enter without one of those components, they wouldn't be able to access. I konw good hackers could still find a way and this is where the IT teams really had to work on from a cybersecurity perspective. But actually, what we've replaced as well is we will be tested. So

every couple of weeks, I'll get emails on all my team will get emails that looks like they're from legitimate people, either in the company or like people we work with, from the global security team checking to make sure we don't open the email or make sure that we don't access the website. And then we have what we call we report phishing. So if we've ever see anything suspicious, and there's a lot of education around that, we did a lot of self service training, we did a lot of sessions with employees around it. And I am in the pharma sector. So when our sector, cybersecurity has always been really important, more so than some other sectors. we always had a lot of protocols and then definitely during COVID with additional ones put in place to make sure that people understood like how you restore your laptop in your home. All too make sure that accidents don't happen and things can't get stolen. if I lose my laptop, or it gets stolen, or if there's any doubt that I can find it, there's a certain protocol for who I activate, react to it so that everything automatically shut down on me. And so even if somebody did find that they couldn't use it.

Okay, so those are some strategies you put in place to protect this from happening Yeah, because it's said to be a business priority at the moment no, because it's risk in businesses.

It is so easy. I made the quip about going to Starbucks but that's the thing you go to Starbucks, Starbucks is Wi Fi is hacked, then you are at risk because your other Wi Fi . There's other things for example, even if I was to go out for a cup of coffee and like my badge from work on, I automatically take my badge off as I'm leaving the buildings but nobody will know what the company that I work for. We will be very conscious physically and online, in relation to what we use our work email addresses for, because if there's things like like we get phone calls, like it's called cold calling where someone would pretend to work in reception of AbbVie and ask for my PPS number for a certain thing. I would know straight away that is not how our process works. And then I would report straightaway to IT. We've had instances where the IT team would track them. We have a global security team. Our Global Head of Security they are exclamatory, right? So, we have very robust procedures, like, you know, around this, and obviously around some of our leaders as well for personal security for them, because they could be high targets. When you think of the products that we manufacture, and what some of them are financially worth in the world, then that's where it's like that security is very important. Our r&d teams would have such tight security. They don't bring their laptops out. So for them COVID was really interesting,

because in certain instances, they couldn't work remotely because of the sort of security protocols and the type of work that they do.

Yeah. Very good. And do you notice recently that the IT teams and cybersecurity teams are like more involved in business decisions?

Yeah, that's really interesting. We are recruiting so like, at the moment, we're recruiting for security engineers that we've been putting on teams in place all over the world. But now, as we kind of come out of COVID, and launch the next phase, we're building out the teams even more. And , there is new rules, it's interesting, I know that there's like some statistic about like a baby born today, there's less than, less than 10% chance that their job actually exists. Our future of work would change so much. But today, like I'm recruiting, tools and platforms specialist, that title doesn't make sense to a lot of people, but within the IT sector, it does. You know, we've like, cybersecurity in nework security, engineers. I was recruiting a Siting Engagement Manager as a manager, and I had never heard of that job before. I learned that they are somebody that will actually connect to someone like me from a cybersecurity perspective they would access what are my unique needs? And what are the particular risks that I might encounter? When I'm traveling and how I'm protected, to make sure that nothing does happen to the company or to me, it is really interesting. And totally different than what I was thinking a few years ago.

Because you are in recruitment, actually. Do you see the automation of jobs as creating new jobs for people instead of taking away peoples jobs.

People are always saying that their job doesn't exist anymore. But that's okay. Yeah. Between retraining and developing. For example, most jobs exist today didn't exist a decade ago, right?Like my role that I'm in right now didn't exist 8 months ago, it was created for me. It would have been a very logical role to have existed, but I'm actually the first person in our organization that has been in my job. My job isn't unique it is just that time has evolved. So therefore our needs have evolved. But I do think people need to upskill, if they stay stegment in just doing what they're currently doing today, that'd be a real problem because that job will not exist forever. the pace of change at the moment is rapid. So people who need to be kind of continuously retrained. For instance, I've gone back to college twice, I've got three times in my life. And I'm not unusual among the people that I work with. We encourage our team so that they're continuously doing extra courses, like not full time

education, but they're doing part time courses, we fund them to do that. So that we're always kind of staying ahead and looking at well, what's the next thing?

So you expect your job to evolve eventually, in an next few years?
Yeah. Since I joined the company five years ago, my job has evolved four times, four times,

okay, well, and do any of the jobs that you ever have don't exist, or are automized now or have you just worked your way up?
I've worked my way up, but I will say, my original job at the company, some of my team are doing it now. How they do it now is not how I did it five years ago. So the tools and technology that are available for them today. And even to the point actually, so I hired somebody to do we have hired a lot in the team in Ireland doesn't last several months, and last September how we would have done something versus how they do it today, due to new technology we got in October. And they are surprised that it previously took so long to do the same thing. And I mean it took me 10 minutes to do it and they think that that's really long. They can now do it twice as quick but at the time we didn't know any different, and that is literally a change since September.

Yeah, because when I was doing my research I read that people are scared of their jobs not existing due to the implementation of robots and there's gonna be no job at all, which isn't going to happen. But when I was doing my research, I learned that the automation of jobs and the introduction of robots into the workplace is going to make a company much more productive, that there needs to be new jobs for people in the future.
For example, in my old job in my prior company, it was in healthcare as well but one of our biggest products was cars. So we made inside of cars. And we had an eight axel robot in one of our sites in America. So basically, the robot was named Berta. Berta had eight arms, and she used to cut and slice parts. With the precision and the speed she was working at, a human being could not do. So if we didn't have her and designed her, then actually, the rest of the factory where we had over 200 employees may not have been able to stay in existence, because a particular company that we were manufacturing for was Tesla. Tesla were bringing out a new car, they needed the speed in order to get the car made to meet their timelines, human beings couldn't have done the job only a machine that was programmed with the same set precision would have been able to do it. If we hadn't secured that contract,

if we hadn't had her for doing her job, then the rest of the work wouldn't have been done. So there's a piece there for its partnership, where it's not automation, replacing people, it's evolving things that get better with ultimately making more career opportunities. Because like our plant, like the financials of that account, everybody else getting paid out of that they were doing other jobs were really, really good and really important, but actually, not having the robot would have been detrimental for us as a business.

Yeah, that's interesting. But going back to no working online over COVID. Yeah. Did you put on any strategies to ensure that your productivity was the same? Or did you notice that there's a change in productivity over this time?

Yeah, it actually increased. Initially, there was probably a dip as people were getting used to it. That was one of the concerns I made coming out of COVID. I said within our organisation that we need to change people's expectations. So for example, personally, my office is in Sligo. So that means I have to commute for an hour eachway so two hours every day. When I go back into my office full time, that's 10 hours of time that lost and minimum 10 hours of time that's going to be lost in a week. Whereas because I'm still getting up at the same time, and instead of me having to get into my car to drive, I would have gone online. So that was an extra 10 hours that the company was getting from me. If I factor that back in that that's going to be a lost, my productivity could potentially drop going back into the office. And so that's why I'm still going to work, at a minimum, three days a week from home. So I only go into the office once or twice a week now. But I think in the first few weeks of COVID, like as people were getting used to technology, there were, and still are glitches, there's still things like the electricity went out in our house two days ago, and it meant that I was down for an hour, it irritated me because I couldn't access anything because I had nowhere to charge anything, and I am an hour away from the office, I couldn't just go into my office. So there is still stuff like that that will happen to people. I think as people got used to particularly during COVID, like having to manage their kids at home, that was really hard because we're trying to manage the schoolwork with the kids and their jobs and that was very difficult in their first few months, until people kind of found it found the routine. So I think productivity changed, but I think was peaks depended on what was happening in their personal lives as well. But I do you think it's interesting, the travel aspect and if they have to commute to work.

Yeah. For example, if your company now I turned around and implemented working five days in the office again, would there be a very negative response?

Interestingly. We did a lot of research which helped us introduce the three day a week in the office. So the flexible policy is that if you have to be in the office for certain jobs, for example if you're making our product, you have no choice but to work in the team room. But for the roles like mine where you can work remotely they made a standard global agreement of 2 days in the office and three at home. We actually surveyed employees and the majority wanted to return to the office but with a more flexible working day. One of the challenges we would have had before COVID is if my kid got sick was home from creche, you had to take a day off because there wasn't any processes or procedures to help and support me working from home. But now if that happens, I want to work because I can still work, so I want a flexible day at hom. Interestingly, over 60% of our employees around the world said, no, actually, we don't want to continue full time remote working because they miss human interaction and coming out of COVID, people miss their personal lives and workplace. It was fine during COVID, we got a temporary office set up. But , now people just want their home to be their home, we don't want it to be like my workplace as well. However, we want flexibility that if we want to go into the office then we can but we can also work from home if we need to. I'm sure there's other sectors, like maybe like for companies like Google, that actually for them their base is in very expensive office buildings in the centre of cities, and saved money on rent by everyonr working from home. They realised that over the last two years does not make sense for them to have these massive high tech buildings anymore, or paying a lot for them but like all their employees can actually work remotely like so there's a large portion of their work that they will never necessarily go back to an office.

Also depends on I'd say, the nature of your job, for example in IT sector, the work is more independent and don't need the office. Whereas the likes of your job, you kind of need to be in the office more.

Yeah. So I do think there are certain sectors that have different ways of working. But for example, I think it's really interesting looking at the technology and how people work, even in restaurants, the increase in ordering online in restaurants where they would never have had that sort of service before. Before COVID, they wouldn't have considered this but during COVID for them to stay open then they had to adopt new technologies.

Yeah. And it's important that companies take the risk of trying technology, because if they don't, they will fall behind very quickly, much quicker than before.

No, absolutely. I recognize that in my particular role there can be a fear around a robot going to take my job, or some sort of automation is going to take my job. The thing is, in most positions, there is still the need for human touch. That's what we need of people. But I think you need to learn adapt and how you use technology and upskill yourself in that respect.

Entrevistado B

Could you give me a brief description of your current role in TCS?

I'm the Principal Consultant and head of IT for TCS, Ireland. So I lead up all the technology operations, engineering and innovation for members here in Letterkenny and across the island that comprises of cloud cybersecurity, DevOps, IT support, all the infrastructure components, and also working with external customers to design new solutions. So I design new IT solutions and deployment in the market.

Okay, brilliant. And has the nature of your job changed over time due to technological advances?

Oh, yeah, of course. I mean, my job would have started in IT management, 25 years ago, where I would have been managing data centers or computer rooms on site within companies. And also desktop users largely based in the office and all the infrastructure around that. With with technology growth, you've seen a lot more mobility of users, laptops, iPads, mobile devices, you've seen a lot more expansion of networks, wireless networks, cellular networks connectivity, and also you've seen computers rooms moving from people's own offices into the cloud or into co located data centers.

Okay, very good. And before the pandemic, were there any options to work remotely, if not, technology aid this

25% of our organization normally worked remotely before the pandemic, so about a quarter of all staff worked remotely on a scheduled basis. So they were in the office one or two days a week, typically, or two days a month. But everybody had remote access, and everybody had a laptop. We went through a change program, probably towards the end of 2014, where we gave everybody a laptop, we eliminated all the desktops in the business, we gave

everybody remote access IDs and everybody secure IDs and tokens so that if they needed to work from home for any reason, or log on late at night, they could do so. So we were ready to go when the pandemic came.

Okay. So there weren't any barriers or anything when the pandemic hit?

Well, no, we do use remote access as part of our disaster recovery in business continuation planning in the event of an issue on site with either the infrastructure, the data centers, or the building, people were used to work from home, and they had an obligation to dial in at least once a month to test the remote access to make sure it was working.

Okay, right. So productivity levels, or any of that kind of stayed the same over COVID, because it wasn't as much of a shock to your company to change workplace locations?

It is so hard to measure, because there's a lot of people who never worked from home. And we're in a sort of software development, consulting and engineering type business. So it's, it's hard to meausre for us but to easier to measure in the call center side of the business where we have people who are on the phones are doing operations support. And we've lots of statistics about work productivity, tickets, calls, messages, turnaround times, and the other more professional parts of the business, it's hard to know whether we got an increase in productivity, whether it stayed the same or whether there was a dip.

Okay. In terms of cybersecurity, it's said to be the biggest risk of amongst businesses in the next three years or so, what strategies have you put in place to improve your cyber resilience?

Yeah, look, there's no one thing that's going to improve your cyber resilience, it starts with employee education. So if you look at the major cyber hacks over the last probably 18 to 24 months, most of them have been targeting both weak infrastructure and poor employee education. So the HSE attack, as an example, was weak infrastructure that left that email and with the rogue attachment, poor employee education that double clicked on that link, and then went through the processes of executing that AgZ and the environment that allowed the hacker in overtime. So a couple of things there is the weak infrastructure is, there are so many elements to cybersecurity from the basics of antivirus protection on all your devices, your endpoint security, your mobile devices, plus your servers, your intrusion detection management, so your actual appliances on the edge of your network that detect intrusions and learn intrusions, and actually download updated information from commercial suppliers to say these are the latest events, your malware monitoring platform, which monitors, the

malware that's out in the wild, as we call it, versus the file changes that it is seeing in the system. You then have to look at things like vulnerable devices that have what's called super user or system admin access. So a common attack vectors, it's called is where bad actors actually attack what's called a jumping off point. And some system integrators and some support companies, the large consultancies, sometimes install devices or appliances in a user's environment to use as a jumping off point to do support. So they log into this device could be a remote access appliance, could be a hypervisor, and then they use them appliances to connect to the customers other systems to do support, or fixes whatever it happens to be, those jumping off points can typically be badly maintained and are quite vulnerable. But the the sort of acceleration of that is that the jumping off point already has superuser access to the job that needs to do so that a bad actor gets into one of those, it's quite a big threat to the company in terms of the they can elevate their own access very quickly and do a lot of damage. Now, what they typically do is they don't do damage straightaway, they stay on there for a couple of weeks. So that's where your data exfiltration monitoring is really, really critical. So you've got your antivirus, you've got your intrusion detection, you got your malware, you got your firewalls, the next thing is to understand if data is getting exfiltrated for any one system. So that's all about pattern management, if you have a Server, Oracle, financials, SAP, Salesforce, and that server normally transmits, four or five gigs a day between users on the internet or between users and remote access, and then suddenly starts transmitting 40 gigs a day, that should be a number one alert on your system to go and investigate that. So why is so much data getting exfiltrated from that server over a short period of time, because obviously somebody has either taken it, or is shipping it or whatever it happens to be. So again, it's not just technology. It's all those systems that you need and they're sort of the basics and good patch management along with, good user education and then really, really good cybersecurity engineering education for your cyber security analyst and your cybersecurity managers that they know actually what they're looking for if something doesn't look right to go investigate. It's a whole package around it , it's not just one thing, it's lots of things.

For employees education, would you send out emails to test them to ensure there are no data breaches?

There are a couple of different things we do. So there's an annual compliance program and a periodic compliance program. So they have to undergo annual cybersecurity training and pass an exam, every employee, it's a basic requirement of employment, that they go through

our system, to actually do the cybersecurity training and pass the exam. There's regular then, surveillance audits for different teams and groups and management. I then will also recertify, my team's access every six months. So every six months, everybody that works for me, all the access they have the systems is sent to me. And I have to go through it all and say "yes, this employee still needs that, another employee still needs that." and I have to verify that and I have to sign it so that the axis is still appropriate for the job they're doing. And then, you know, as you go through them, there'll be certain scenario emails sent to you, so phishing emails, and they'll test whether you're really reading the stuff or not and if someone clicks the link, you have to go back and do another course. So we'll send out the email. If you happen to click on the link, we've got a phishing button on our email platform, you're meant to report that if you see it, so you click on the phishing button, that email gets taken away out of your inbox. We then go through the headers and footers on email, try and source the origination, block future emails from that location, things like that. But if you click on email, and it is a scenario email, we will actually make you go back and do a course then.

Okay, good. And when people are working remotely, do you have some sort of like, extra security? Did you use private networks or anything to protect your systems?
Yes, there are two different things depending on what system your accessing so we use a platform called Zen scaler, in the cloud, which then monitors their internet connectivity, their access so that we only connect to trusted sites, blocks everything else. We also have VPN tunnels for private corporate applications. And also we use multi factor authentication for all application access. So when you log in in the morning, it's a multi factor authentication pin to your phone. Sometimes we randomize it, so it allows you to open an application, sometimes it'll send you a text, we don't tell people what we're doing. So as if somebody has intercepted their application or intercepted their phone, we can redirect around that.

Okay, brilliant. And since technological innovation is occurring at a rapid rate, and jobs are being automated, do you think that your role will continue to evolve in the future?
Yeah. Look, I think what you're gonna see in automation is the automation of... like everything in computer science or computing since the 50s and 60s, the automation is going to automate the tasks that are best automated, there is no point in trying to automate a task where you do require a large amount of human intelligence or behavior, it's not going to

work, it tends to be very, very costly and largely unsuccessful. Where you'll see automation play a significant role in those mundane repeatable tasks, which are very processed driven, can be measured pace, and are best done by a machine. So if you think about some of the technologies that are playing a role there in rpa, remote robotic process automation, where you can teach a computer to do a particular macro type task, and then every process that comes in that meets the criteria of this task, the computer just does it. That's a really, really good way of doing it. Similarly, in testing software, you know, you can apply large bodies of automation that including the cybersecurity work, you know what the vulnerable threats are, you know where the quality holes are, you can use automation, and use systems to really aggressively test those vulnerabilities in the system, that a human can never test at the same pace. However, the outputs of those reports or the outputs of that testing, a human does need to remediate them, because the fix could be completely different for two different systems. So it's important that we use humans and technology in the right proportions to do the right things. Because, you know, a computer is never going to be able to know the nuances or the context of why software code was developed that way, and may inadvertently fix the vulnerability, but make the software useless. So do you need humans to be able to say, Well, hold on, I need to fix the vulnerability, but I need the basic function and the software still continue to work.

So it's going to be used to speed up the process in many job?

Where automation and artificial intelligence, particularly in cyber infrastructure management engineer, data center usage, where artificial intelligence and automation has a key role to play as highlighting those issues that you should address. So a computer can quickly assistant and can quickly analyze, based on all historical operations before, this is a real threat, or based on all historical failures before this is, I can predict this is going to be a failure, we look at the last 3000 tickets that were put in against the system over the last four years. If you let this Event Manager Go, or this this space, or this SQL Server running a tablespace, the system is going to go down. And to put that to the top of the queue for an operator and say, Look, you need to address this before the system goes down. That's where artificial intelligence and automation has a huge advantage. Because there's so much noise in event management, and so much noise in IT, all these different observability platforms and systems that we use to manage infrastructure, e commerce, transactions on the web, people buying stuff, there's a lot of noise. Artificial intelligence and automation can actually

distill a little bit of that and take away what sort of that automation can deal with, and actually put the important stuff to the top.

Okay, so would you say that, like a lot of people are scared that robots and automation of jobs are going to actually like, ruin or take away jobs for humans, but really, it's going to increase productivity and then create more jobs?

It's going to increase workforce, it's going to increase jobs. I mean, if you look at that, actually, the exact same argument was used in 1959 and 1961. The IBM mainframe was coming on stream and they were looking at automating the people are used to put the punch cards in the machines or the people used to do tabulation and things. But it spawned a brand new sector of commerce, like computer science, computers technology is now one of the most foremost businesses in the world. It didn't actually take away jobs, it actually completely changed the way we work and completely changed the companies and completely change the world of work. So rather than actually getting the jobs of millions and millions of jobs over the last 40 or 50 years, the exact same is true in the next evolution of technology.

Yeah, exactly. So people are in their current jobs are just gonna have to upskill or retrain in order to keep up with the technological changes.

Correct, I think there's two different elements. There's the people that are gonna have to upskill and retrain and cross train. And then there is a suppose a gap right now for people have come in to the computer science world, digitally native. So they're born into technology, they understand how to use technology, they're great users phones. You know, you can use a phone, an ipad, can use a screen and can use Zoom but have no understanding on how it works. You know, whether at the disc layer, the IP layer, the processing layer, the silicon layer, networking, they have no clue. professional consumers and users if it. And then they do grow into technologists, but they're born digital. They're developing on the cloud. Technology is abstracted for them. So there's another wave of people that do need to be trained and upskilled and how to make all this work and how to continue to make it work. And there's a skills gap there as well. So it's very skills gap at the top in terms of digital and there is an equally big skills gap at the bottom in terms of engineering expertise, and building all the core components of the foundational components to make all this stuff work. Even the cloud, people talk about AWS or Google or microsoft, they're just servers and someone else's data center. So there's no real rocket science to them, they are just servers racked in a

rack powered by electricity connected to the internet, cooled by air conditioning. The magic is in the software and the hypervisor and the hyper scalars. But I think we're seeing that gap and both the high end and the entry level right now that does need to be plugged.

Okay, good. I think we've covered everything there.

Cool.

Entrevistado C

Give me a brief description of your role in Equifax.

I work as a senior product owner in Equifax. So that means I'm responsible for a particular system that the business use in credit transactions in the US. Basically, it's a system used by people in call centers to contact and verify candidates income, expenditure and assets. So, in the US or anywhere else, banks will use credit bureaus to get a credit history of people who are applying for loans, mortgages, personal loans. And they need to be certain that those people have good credit. So they'll check the income and expect the income, deployment details and the asset details that the client gives systems and the employer. So basically, we're like the middleman between between the banks and people who were borrowing money.

Okay, very good. And has the nature of your job changed over the time over time due to technological advances?

Yes, it's changed very significantly over the last number of years. Mainly because most businesses have now moved into the cloud. So the business I'm working is using Google clouds. So Google Cloud is a massive change in terms of getting away from traditional databases, everything is backed up in the cloud. Security is managed by the cloud and it's a huge kind of transformation in terms of how businesses operate and how they are structured.

And before the pandemic, were you able to work remotely at all. And if not how to technology to change for you to work remotely.

Equifax didn't really didn't encourage remote working. But I started, they believe more in teams being co located and people coming into the office. But when the pandemic hits, that obviously changed dramatically. And they were forced to roll out remote working. So what the amazing thing is that it works really well. So people can log in from from home. And you log into a dedicated server. And obviously, you have to do dual identification, which

will involve your phone and your computer, it's quite safe to say your login your login to the virtual public or private network. So you know, nobody can steal your data. It's very secure. So the security is monitored by the cloud infrastructure, essentially. That's been working for the last couple of years. And it's very successful.

And it's going to continue that way for the foreseeable?

I think it has to continue because if it doesn't, people will not be happy. Most people have found it works very well for them in terms of their personal lives, much less to travel. So it's much more suited to people, quite a few people have moved to different locations in different parts of the country because accommodation is quite expensive in Dublin. So they would be very hesitant going back to the office ending like full time, and the company has had to recognize that because if they don't recognize people will leave.

Okay, very good. So were there any barriers to technology when you had to change from office work to remote working? And you've told me that there's measures put in place to ensure there are no data breaches by using private networks?

Yes. So Equifax kind of suffered the biggest ever breach of clients personal information, a number of years ago, about four and a half years ago, where a vulnerability was was detected in the system and hackers were able to hack in and steal the personal data of 150 million Americans. That breach was a very high profile, ended up in Congress. And since then Equifax had to go on this transformational process, which is to move to the cloud. So security will be managed in the cloud to avoid those type of breaches in the future. So these big these big companies like Google and Amazon have huge advantages, and huge teams looking after security, the security, that source to these companies. And everything is encrypted, encrypted means that nothing is sent in plain text, everything is encrypted, and then unencrypted, using various algorithms. So nobody can steal data easily now.

Yeah, it's meant to be a business priority because of the increase of cyber attacks during the pandemic.

Absolutely, yeah.

One thing to note is Equifax has sought to build a cyber- aware culture. All the best IT defences won’t protect your business if you don’t train and educate staff to guard against potential attacks and follow your cyber rules. You need to establish a regular safety and awareness engagement program using a combination of strategies like newsletters, eLearning, new starter briefings and a manual outlining what staff are allowed to do and not do. Conduct controlled exercises that practically demonstrate the different ways hackers

might try to breach your secrets. Make your people aware that this is a vital issue for them to be conscious of both at work and home.

And were there any ways that productivity was stabilized at the beginning when you started working remotely?

where I worked, it was a learning curve, but not a huge learning curve, because most people are quite technologically aware and in general a lot of people are very self sufficient. So they quite liked working on working remotely. And we were initially using video conferencing on off but after a while, people just they found it a bit intrusive so we stopped using that. So it's, it's audio conferencing, but it works very well.

Good. Since technological innovation is occurring at a rapid rate, and the introduction of robots into the workforce is expected to automize different rules, do you think that this will affect your role? Or do you expect your role to evolve in any way in the future?

My role is only going to evolve, because I'm a product owner. So I'm looking after the business requirements and what the business wants and I do expect changes in terms of other roles. So like development roles to the increasing automation of the calls, and SRE's which is type of responsibility engineers, these are the people who look after the web infrastructure. So for example, Google, we will have an SREs who are very skilled, and they are completely new role. They are looking after maintaining and keeping the infrastructure up and running. In terms of developers, automation is going to happen. And certainly in terms of the business people that I'm dealing with, 100%, they're going to face challenges where a company will try to automate those processes. So for example, the system I explained to you about, for people in the call center, are reaching out to employers confirm people's incomes, expenditure and assets, is done by people in a call center, they're supported by technology. But the goal is to essentially replace those people with machines, with automation. So it'd be much less of those people in the future. That's what the company is planning for.

And do you think when these jobs are automated, that it will increase the productivity and then create new jobs for people? Or will there be less jobs available for people in the future? I

I think new types of jobs, new types of jobs that the titles haven't even been identified yet. Yeah. So for example, in the last number of years, in IT, a whole plethora of new job titles have come along, like SREs, like product owners have moved away from, you know, having developers, analysts, project managers, program managers that were previously there. There is likely to be a lot more job titles like, artificial intelligence is huge. On that, there will be

a lot of new roles there. But the educational background will need to be high for those type of roles, so it will be tough, some people will find this easier than others. They will have many many opportunities, others will have to relearn which is difficult.

Exactly I think that's everything thank you so much.

Entrevistado D

1. Could you give me a brief description of your current role in Abbott.

I am manufacturing manager in Abbott Diagnostics in Longford. My current role is in projects introducing automation and new technology into manufacturing. The main project I'm leading is the introduction of a Manufacturing Execution System (MES) which includes electronic batch records (EBR).

2. Has the nature of your job changed over time due to technological advances?

Yes, as above, pretty much my job is to introduce new technology so maybe if there weren't any new technology, I'd be out of a job!! When I started as a manufacturing manager over direct manufacturing, there was a lot of manual steps and inspections involved in the process. This leads to a very slow and labour intensive process with high risk for human errors. This manual process causes a lot of work for a manufacturing leader and is not optimal for a factory that is growing very fast.

3. Before the pandemic, were there options to work remotely? If not, how did technology aid the change from office work to remote working?

Yes, I worked remotely 1 day a week prior to COVID but I was probably an exception. 95% of employees would have worked on site prior to COVID. However, I chose the day that there wouldn't be any meetings to attend and it was to focus on project work that didn't require interaction with anyone else. Once COVID happened, most indirect employees (i.e. not directly involved in manufacturing) had to work from home and technology was used extensively to enable this. We used Cisco WebEx initially but changed to MS Teams after a few months as it was a better experience.

4. Were there any barriers in technology when having to change from office work to remote working? Were there any measures put in place to ensure there were no data breaches?

Initially Cisco WebEx was used but the video and voice calls were not good quality so we moved to MS Teams. I'm not aware of measures put in place to avoid data breaches but I'm sure our IT department were working around the clock to ensure we had sufficient cyber security.

5. Cybersecurity is said to be the biggest risk among businesses within the next 3 years and should become a business priority, has your organisation put any strategies in place to improve cyber resilience?

Yes, we have awareness training for all employees which gives examples of simple errors which could lead to major breaches. We also have "phishing" reporting if we suspect an email is suspicious. Also, as I'm involved in the introduction of new equipment and IT systems, I know there are strict guidelines on adding new equipment to our network. In addition, we are currently going through remediation of some of our older equipment to ensure that they do not pose a cybersecurity risk.

6. Did you have to rely more on technology when having to work during the pandemic? Did your workplace respond positively or negatively to this change?

Yes, all our meetings moved to online via MS Teams so technology was key to successful running of the business. In addition, on the project that I am on, we went through a full scope out of user requirements and vendor selection all through MS Teams. Prior to COVID, this would have involved many trips back and forth to the US. I didn't have to travel once and we achieved all our timelines.

7. Did productivity levels change when the company began to work remotely? Were there any different practices to stabilise productivity during this time?

I believe productivity increased at this time. This would have been partly due to the fact that all social activities were closed/cancelled and employees spent more time working. We did re-energise our reward and recognition program to recognise employees' change of work circumstances. Employees were also offered resources so that they could complete their work adequately from home.

8. Since technological innovation is occurring at a rapid rate and the introduction of robots into the workforce is expected to automise different roles, do you think that this will affect your role or do you expect your role to evolve in the future?

Yes, as I've mentioned, I'm heavily involved in the introduction of automation and new technology into manufacturing. I believe that there are still major advances to happen with

automation, collaborative robots, artificial intelligence, augmented reality and data analytics. For my role, I'd like to stay in touch with new technologies and bring leading edge technology to Abbott. For manufacturing managers or team leaders over direct manufacturing, I believe new technology will change their role from fire fighting and dealing with human error to being proactive and making improvements in manufacturing efficiency through data analytics.

Entrevistado E

Could you give me a brief description of your role?

I am a regional ethics compliance officer. I work in a company that has 53,000 employee's all over the world. I think they have presence in well over 100 countries. We specialise in carrier brands. It is mainly associated with air conditioners but, we also have fire and security refrigeration including refrigerated lorries for food trucks. We make all sorts of refrigeration equipment for industrial refrigeration. I'm involved in the fire and security side so we do access control, security cameras, fire detection, fire suppression and ethics and compliance. My role is basically making sure that the employee's comply with our code of ethics, that we don't break the law. And I do training and investigations in corruption, anti - competitive practices, respect in the workplace; I would even look at harassment cases and sexual harassment, bullying and discrimination - anything that is unethical in the company. I am responsible for Europe, Middle East and Africa, for the fire and security business, making sure that people comply. It's really interesting.

Okay, very good. And has the nature of your job changed over time due to technological advances,

More organizational changes, subcontracting, back end, finance tasks, and accounting tasks. Rather than having people on payroll, subcontracting those to third parties, what it does is it loads segregation of duties as well, which is a benefit to the company, as well as a cost saving regarding technology, we're always looking for new new ways to facilitate processes. We've got a lot of workflows, to control, things like giving company gifts. What else? We have lots of ERPs, we grew as a company that's based on acquisitions, so we've lots of different ERP system, systems to control, stock inventory, you know, are trying to standardize those.

Did productivity stay the same during the pandemic?

Well, I used to work two days from home anyway and now with the lock – down, I'm working all the time from home, which is the biggest change. I had a home office anyway in the living room, so I have my second screen; I need to work with two screens. I have two screens at work and I have two screens at home. I have the set up, so that was fine. Also, we had a VPN, a virtual private network, so I can access the servers from home with no problem and securely. I think the biggest change is that when I work from home, the kids are at school, that's fine, but working at home with the kids not at school was a completely different challenge. It was much harder because the kids were being given homework, if it wasn't for my partner, to be honest with you, I wouldn't have managed. I mean, they're not organized or methodical about doing it on their own and they need a lot of help, you have to send all that stuff back by email.

So I guess the positives are not needing to commute to work, you know, saving almost a couple of hours every day. Also, if I get up early, say, six o'clock, then you can get a few productive hours in before the kids get up. I kind of had to adjust the work day to try and be efficient. So getting up before the kids and then getting a few hours done so then when you are interrupted during the day it is not so important because you have got a lot of work out of the way. And also, my job requires travelling. We have harassment investigation in the north of Spain, and I have to manage that next week, interviewing people over the phone, and that's going to be difficult because when you're investigating, it's really important that you have personal contact. You know, I can do trainings by WebEx, I can communicate by email, but when you're investigating harassment, you know, it's very important to be face to face with the victim and the alleged harasser because you can get a lot from their body language, about if they are being truthful, and things like that. So that's going to be a challenge. But it will be interesting as well.

Very good. And before the pandemic, were there options for you to carry out work remotely. And if there wasn't tied to technology aid to change from office work to remote working?

Okay. We did have a jornada intensiva, before COVID, where we could work in the summer, and we could work from home one day, a month, I think it was, but yeah, no HR, the business was very much against the working from home, except a few in a row where you need to be meeting with customers or need to be out on the road. But any office based job to company was very much in favor of people being in the office, except for that exception during the summer where we had that opportunity to work from home a little bit. But since COVID

Yeah, that's changed a lot. And technology wise, no, we were using telephone audio at the time, and zoom. We used WebEx, which is was really rubbish. You could share a presentation, but we wouldn't normally switch on our cameras. So I think COVID introduced this teams and their zoom stuff where you're seeing lots of people on the screen. But before that we never had meetings when we were working from home in that way. It was a lot more old school.

Yeah, and implementing technology such as the likes of teams and stuff, did it make sure that user as productive as us could be in the office. Yeah?

I think so teams is great. It's it's got set backs, but I think the positives outweigh the negatives of teams, for sure. For collaboration, that's the whole SharePoint, you know, concept behind it means you know, you can you can work on files together, and from different locations, make make updates. And if there's a mistake, you can roll back versions, which is really, really handy. If you accidentally delete a load of slides, because it's on SharePoint, it's got the whole history of the document. Okay. So, yeah,

were there any barriers to technology when changing from office to remote work? Like, for example, were there any measures put in place to ensure there are no data breaches or did use private network?

Yes, yes, yes. Before we were using Cisco, for the VPN, Operation worldwide, Z scalar for the entire business, and they did that in record time because of COVID. So yeah, we use Z scalar. For secure access. We've had the you proactive this. We've got a cybersecurity team that are very proactive. They do a lot of training. They send us fake emails to see if we're sleeping, you know, saying your deliveries about to arrive and it looks realistic, and they they send spam as well, you know, to raise awareness within the company. But they'd be doing that before COVID, too. But yeah, with Russia, were pulling out of Russia, they were getting cyber attack attempts almost daily, if not daily, they were just frequent.

Okay. And yeah, because of this increase in cyber attacks recently, it said that cyber and cyber security has to be a business priority now, as your organization put in any other strategies to improve your cyber resilience?

Well, we have this corporate with the the code, information security officers where we have those roles. And we have that team, which is a lot more visible in the past 12 months than it was before. I think the GDPR brought in, you know, the main sort of policies and processes

to protect privacy, which isn't the same as cybersecurity, but you know, they kind of overlap in a way. I'll be honest, I don't work and the technology cybersecurity side of things

But what they be more involved in, like business decisions and stuff within the company than they would have been before.

definitely yeah, definitely. Yeah. Okay, we have a whole cybersecurity function that reports right up to work orders. The Privacy function, which is more the legal department, because there's legal implications if there's a data breach from our side, with personal data under GDPR, other privacy laws.

Okay, very good. So since technological innovation is occurring at a rapid rate and introduction of robots into the workforce expected to automate some jobs, do you think this will affect your role are expected to evolve in any way in the future?

Yeah, we had a guy that was working on bots, for the legal department and factors, the software now that where you can you can ask a legal you can make a legal consultation, and because they have a database of the laws, you can have artificial intelligence, understanding, you know, at least basic questions and giving you answers without needing to consult. That's definitely something that I can see coming. Yeah, currently, it's just people. I think when I investigate, I think that the investigation side, it's, you still you always need people to do that, I think, you know, depending on the case, but almost always because somebody's done something wrong. And you also need to understand, you know, why they did something wrong as well as you know, was it for personal benefit, etcetera, etcetera. So, you have to interview people, I can't imagine about taking place of taking the place of an investigation team investigating harassment, where there's perception of harassment, you know, how serious that was. There are two sides to the story. And, you know, two people in the rooms that did happen, it didn't happen, and there's no witnesses and one word against another that's it might be, yeah, something that will come in the future, but I don't see it coming you know, for the next 15 or 20 years. That's not something next year.

So you feel that you kind of need people to carry on your jobs.

Yeah, we're training people on compliance. Face to face is so much more effective. Even using technology, and I've started traveling again your relationships change with people once you've actually met them in person.

So how was your job affected in this kind of side of things between traveling and having the face to face meetings during the pandemic when you couldn't have those face to face meetings?

It made me realize that I totally miss judge people by using teams meetings, you know, for whatever reason, they might not communicate as well. You know, many countries do we do business and I have no idea but we're global. And there's a language barrier and when you're with a person with body language, you can really get a much better sensation for what they're trying to say I totally misjudged one of my colleagues, you know, I thought she was not into the job. I went to Hungary asked her, you know, do you like your job? You know, that was the first thing I said. She says, I love it. And I couldn't get that through the online conversations we were having. And then I spent three days there and by the end, I saw exactly how much she loved what she was doing and what she was doing, and she wasn't able to get that message across. Because of language, mainly, I think because she didn't know me maybe, um, maybe expectations. She didn't know how to build trust and yeah, so ya know, that's a big eye opener for me. For sure. The physical contact I think is essential no matter what technology we have especially for building successful teams and businesses. Really feeling my boss was here for three days. You know, I'm so motivated after she's been here that you know, she can't do that on the phone or over video.

I think your job is more effectively done in real person rather than remotely?

Yeah, yeah. Not a lot else the subcontracting of non-essential services to third party is a big thing we're doing but it's not state of the art technology. It's just a company strategy.

Entrevistado F

Could you give me a brief description of your role?

Yeah I am a senior director of corporate security in Twitter.

Has the nature of your job changed due to technological advances?

Yeah due to technological advances and the use of technology to commit crime or threaten people, it has been made so much easier due to technology. Like, instead of meeting someone on the street and abusing them. Now, there's a huge sway of people that just abuse people online, as you know, whether it's on Twitter, or on Facebook, or it's on Instagram, whatever it might be telegram.. people use technology, internet, and various platforms to send abuse or threats online. And one of the things with that is, as much as that's not as

confrontational as a physical threat, when you meet someone on the street, or in a bar, or you're speaking at a conference, and someone might abuse you, or if somebody harasses you when you are speakers. It does have an effect on people because it's cyberbullying. Even for kids at school. The old thing when when kids went home from school, if they were being bullied at school, or at least they were at home they weren't being bullied. Whereas now, because of Facebook, or whatever, kids are still getting them when they're at home. And the same way for adults and it is more sustained because of technology.

Okay. Before the pandemic, did you have the option to work remotely at all? And if not, how did technology aid the change from office work to remote working?

As a company, pre pandemic, you can use this as a reference point, so Jack Dorsey who founded Twitter and was was the CEO of Twitter up to recently had decided, while I was in Africa with him for a few weeks and part of his experiment was visiting Africa. He started to actually move to Africa, to work as the CEO of two companies, Twitter and Square, to prove that you can work from anywhere. So like, this was in 2019. In autumn 2019 we were in Nigeria and Ethiopia. So he already had come up with the idea and he was going to prove that you could work remotely from anywhere in the world. He was an advocate of this, and he was going to prove that it could be done by he actually living in, for example, Lagos, Nigeria for three months, and being the head of two companies, two major companies and working remotely. So that was going to be using technology, which is his life is technology. So that's one point - World technology leader Jack Dorsey was already promoting remote working pre - pandemic.

So you had the option to do work remotely before the pandemic?

Yeah, absolutely. So basically, within a week or two of the pandemic starting in March 2020, so let's say by April, Jack Dorsey announced that they everybody can work remotely, forever, literally, that's the quote from Twitter, so if you work for Twitter, you can work remotely forever. So it wasn't like for the pandemic because nobody knew that how long the pandemic was going to last. So he used his already predisposition to remote working during the pandemic to prove his earlier point. That idea still exists in Twitter. I know there's some managers, and this happens every company, some managers of people will refuse people the right to work remotely. But in general, if you work for Twitter, you can apply to work remotely and you'll likely be allowed.

Okay. Very good. Are there any barriers to working remotely? for example, were there any, like strategies put in place to make sure there's no data breaches for working remotely.

So that's a good point. So one of the things I like is if you're if you're going to be working remotely certain countries in the Middle East, certain countries in Asia. So the problem is, if you can be hacked, or compromised by a non state actor, which is, a hacking group, like the hacking group that hacked into the HSE, in Ireland last year, that they're not non state actors. And I'll come back to that a second. But one of the other ones is the state actors, so countries like Turkey, Saudi Arabia, China, any country, America, any country with high sophisticated technical ability to compromise and hack and intercept people's technology. So for years and years and years, nearly every country had the capacity to intercept people's phones. Originally, it was like landlines, which is easy. Then in mobile phones, a lot of that is done legally, it's done in Ireland, people's mobile phones are tapped for Crime Prevention and terrorism reasons and that's done with permission of the government. So now that technology has expanded so much that they can hack your email, or they can act as your email, every email you get, they can get. So this is the long winded answer to your question. if you're in a country, where it could be like a non sophisticated country, like I mentioned, Ethiopia, or it could be in a really sophisticated country, like Saudi Arabia, or China, where that technology is being used. And that's why remote working is an InfoSec, from an information security point of view. So like in our company, there's two main security teams. One is the corporate security team, which has physical security, so offices and people traveling. And then the other major part of security is information security called InfoSec, which is looking at your laptop, whatever you're using slack and everything we use, how that can be compromised, for the benefit of others. Some of its state actors, some of it not state actors. Definitely cyber information security, cyber security is a major factor in deciding whether a person can work remotely, and so that their Wi Fi systems are secure.. So basically, it's bringing it to a level of security that people can tolerate, because if someone targets me, no matter what country I'm in, that's where the state wouldn't be involved in, in hacking into companies like us. But another company, let's say a startup company who wants to mimic on Twitter, those are what Facebook do. They can hire experts to try and hack some of the engineers on Twitter. So therefore, if that engineers working on a remote Wi Fi or something like that, they might say, "Let's go after this guy and try and figure out

what Wi Fi he is on." And then that wouldn't be as easy to do if he was working in a secure building with a secure Wi Fi system.

Okay. Very good. So that is the biggest risk to companies nowadays is cyber attacks. Do your cybersecurity team put in any measures to make sure that you avoid these attacks?

Yeah, so we have like two step verification and on everything we do. That's basically using really secure passwords.We've tested passwords that have to pass a really high level of testing, our passwords have to be very strong, and that's only one part. And then we use YubiKey. It's basically a little black key that fits into the side of your laptop. And there's a little thing for your fingerprint on this for fingerprint verification that you touch. At a certain time, when you're doing the two step verification, it gives you the most touch the YubiKey. And there's there's a lot more to it than that but it short that is what you do.The two step veerification is a standard in our company.

Okay, yeah. I will ask one last question. Technological innovation is occurring at a rapid rate and adoption and the introduction for robots in the workforce is expected to automate different roles, do you expect your role to evolve because of this? Or change in any way?

I will say that my role but the role of information security slash cybersecurity specialists in companies in states like what I keep referring to both, whether it's the Department of Foreign Affairs in Ireland or whatever the State Department Americans are in private companies like Twitter and Google or Facebook, the role of information is not cybersecurity. People will surpass I think the role of physical security people like me. So really, the reality is there's going to be much more roles and much more emphasis on budget. So like in the future, let's say, people in our company , we've got so much budget for security and shouldn't be putting it half and half and one is physical. One is cyber, or should we put more 75% in cyber because the likelihood is that budgets in companies and in states will move towards will move towards putting more into cyber security than they will into physical.

Very good. I think we can leave it there.