GRADO EN COMERCIO

TRABAJO FIN DE GRADO

“Comunicación empresarial, internet y redes sociales: propuesta de Guía de buenas prácticas para empresas y trabajadores”

Eva Gómez Martínez

FACULTAD DE COMERCIO
VALLADOLID, JULIO 2021

FACULTAD DE COMERCIO
Universidad de Valladolid

UNIVERSIDAD DE VALLADOLID
GRADO EN COMERCIO

CURSO ACADÉMICO 2020/2021

TRABAJO FIN DE GRADO

"Comunicación empresarial internet y redes sociales: Propuesta de Guía de buenas prácticas para empresas y trabajadores"

Trabajo presentado por: Eva Gómez Martínez

Firma:

Tutor: María Inés Sanz García

Firma:

FACULTAD DE COMERCIO

Valladolid, 13 de julio de 2021

Índice

Contenido

Comunicación empresarial internet y redes sociales: Propuesta de Guía de buenas prácticas para empresas y trabajadores

Eva Gómez Martínez (eva.gomez@alumnos.uva.es)

Grado en Comercio

Palabras clave:

Internet; redes sociales; teletrabajo; ciberseguridad.

INTRODUCCIÓN

A lo largo de la historia, la forma de relacionarse de las personas, instituciones y de las empresas, cambia tanto en sus métodos como en sus contenidos. Y este gran cambio ha tenido puntos de inflexión en determinados momentos de la historia; uno de ellos es el momento que estamos viviendo desde el siglo XXI, y como punto fuerte el año 2019 que comenzó la pandemia en la que estamos inmersos. La forma de relacionarse que, en esta ocasión, y como consecuencia de la COVID-19 no ha sido una opción, sino una necesidad.

Atravesamos un momento complicado, debido a que vivimos una pandemia que ha transformado la forma de comunicarnos y de trabajar. Gestionamos la comunicación a través de internet (en la web de cada empresa), pero de manera prioritaria y fundamental en las redes sociales.

Gran parte de las instituciones y empresas habían comenzado el proceso, en este nuevo medio de trabajo y de publicidad; pero añadido a esta circunstancia se han tenido que adaptar a relacionarse con sus propios trabajadores, de forma telemática. Todas ellas, como decía ante todo pymes, y por supuesto las que han sido capaces de adaptarse a esta nueva forma de trabajo.

En los últimos años, la introducción de internet en el ámbito empresarial y comercial ha sido fundamental, obligando a las empresas que buscan subsistir a llevar a cabo cambios profundos, buscando adecuarse a los nuevos hábitos tanto de consumo como de relación profesional como consecuencia del desarrollo de las Tecnologías de la Información y Comunicación (TIC's).

La importancia del uso de internet es relevante, debido a que se amplía enormemente, el número de posibles usuarios, inversores, empleados, clientes, pues muchas son las empresas que se han volcado en hacer de internet su medio de trabajo, de publicidad, su escaparate, y se ha transformado de forma intensa y profunda la forma en que las empresas publicitan sus productos, sus técnicas de venta, como realizan sus estudios de mercado, las promociones.

Internet y las redes sociales, son un medio muy cómodo, rápido, sencillo y barato para captar un gran número de potenciales clientes, que antes era impensable y mucho más costoso e incierto. Han facilitado mucho este tipo de trabajo de publicidad y captación.

No obstante, el uso de las nuevas tecnologías, que en principio parecen establecerse con un carácter neutro en cuanto a su uso, puede conllevar dos aspectos, el uso debido o buscado con su implementación, pero también un uso indebido de las mismas.

A pesar de los avances en las formas de comunicación y las nuevas formas de trabajo, es un hecho que la pandemia de la COVID-19 ha acelerado y variado las formas de comunicación y de trabajo en todos los ámbitos de la sociedad, siendo interesante observar la manera de usar todas las herramientas a nuestro alcance.

Son numerosos los estudios que se han venido publicando sobre el avance de las redes sociales y su calado en todos los ámbitos de la sociedad, tanto a nivel nacional como internacional.

Varios son los estudios sobre redes sociales, a nivel nacional como internacional. A nivel nacional tenemos la ONTSI, el IAB, y la Asociación para la investigación de los Medios de Comunicación. Por el lado internacional, el número de estudios es amplio, debido a que muchas universidades y entes los realizan de manera regular. Tenemos el ejemplo del ranking que realiza The Times Higher Education World University Rankings, en la que se crea una lista con las universidades, más de 1200 que utilizan redes sociales para conectar con sus alumnos. O como por ejemplo la Science Direct (revista de ámbito científico, que recoge abundantes estudios sobre este fenómeno).

El presente trabajo se basará en la realización de un cuestionario, abierto a profesionales de diferentes sectores de actividad y la elaboración de dos guías para un uso racional y ético de las redes sociales en el trabajo, tanto desde la óptica del empresario como desde la del trabajador.

Como forma de abordar la parte final del trabajo, y parte no menos importante del mismo. Además de la encuesta y como resultado en cierta manera de la misma, resulta interesante realizar dos guías prácticas de buen uso de las redes sociales en el

trabajo; con ello se intenta desde una mirada de trabajador y como usuaria de estas redes, de lo que podría ser el uso racional y ético de las redes sociales en el trabajo, desde la mirada del empleado como la del jefe. Lo que pretendo es dar un enfoque eminentemente práctico.

Con este trabajo se pretende hacer una reflexión, sobre lo que se considera normal y lo es, es decir, en prácticas normalizadas poco respetuosas, y en lo que no se hace correctamente y se deja pasar por las posibles consecuencias.

Para ello, en el capítulo primero es interesante hacer un breve recordatorio sobre la historia de las redes sociales, los estudios que se realizan sobre las mismas, y dentro de este mismo capítulo se incluye también la manera en que las usamos como individuos y/o empresas. Como continuación y para seguir en el capítulo segundo, como se manejan, la comunicación interna y externa a través de internet, además de las tendencias que se toman como guía o referencia, y las que llegaran.

Cambio de tercio en el capítulo tercero, nos metemos en terreno interesante con el cuestionario a las personas que de forma voluntario han querido colaborar, y han dado su opinión, ventajas e inconvenientes, que se incluyen en el capítulo cuarto, en el que además es conveniente reflejar por supuesto los valiosos consejos que, tanto en el trabajo, como en las guías que forman parte de este trabajo.

Para finalizar el capítulo quinto explica y resume, lo que ha supuesto este trabajo, lo que no se ha podido incluir, y lo principal, todo lo aprendido.

Agradecimientos.

En primer lugar, es para mí muy importante agradecer el esfuerzo y la paciencia, a cuatro grupos de personas, diferentes y relacionadas entre sí.

Familia, que siempre aporta consuelo en los momentos complicados.

Amigos, personas sinceras, y que siempre quieren ayudar.

Profesores, que siempre están disponible para ayudar en la investigación y búsqueda.

Compañeros de trabajo, que siempre han estado pendientes de mis estudios y de mí.

Todos ellos son muy importantes, porque he compartido información, pesares, diferentes puntos de vista, frustraciones, etc.

Gracias a todos por la amabilidad, cariño y la paciencia que han demostrado.

1. LAS REDES SOCIALES Y LAS APLICACIONES DE MENSAJERÍA

1.1. Historia breve de las redes sociales

Para entender el fenómeno de las redes sociales, es recomendable hacer un breve repaso por su nacimiento y evolución, partiendo por supuesto de la madre de todas ellas, Internet.

La llegada de internet se produce hace aproximadamente siete décadas, en los años 50, comenzando la Guerra Fría, con el enfrentamiento de los extremos del mundo, Estados Unidos y la Unión Soviética.[1]

Como toda batalla de poder, fue liderada por la tecnología e impulsó la invención de avances tecnológicos. Entre esos avances el más importante se produjo en 1958 los EEUU fundaron la *Advanced Researchs Projects Agency* (*ARPA*) a través de la Secretaría de Defensa. El ARPA se formó con más de 200 científicos de alto nivel y un gran presupuesto. Su objetivo era crear comunicaciones directas entre ordenadores para poder comunicar las diferentes bases de investigación.

En 1967 ya se había hecho suficiente trabajo para que el *ARPA* publicara un plan para crear una red de ordenadores denominada *ARPANET*, que recopilaba las mejores idas de los equipos del MIT, el National Physics Laboratory (UK) y la Rand Corporation.

Años después el sistema evolucionó, y poco a poco más usuarios, diferentes de los originales, comenzaron a comunicarse por correo electrónico, a partir de 1971, un ejemplo es el Proyecto Gutenberg (la biblioteca online gratuita).

Fue a partir de los 90, se hizo pública la red de internet global, con el World Wide Web (lo que, comúnmente conocemos como «www»), y así surgió Internet.

[1] https://marketing4ecommerce.net/historia-de-las-redes-sociales-evolucion/

A partir del conocimiento y acceso a internet hemos experimentado cómo este mecanismo, generó un punto de inflexión en todas las sociedades, principalmente porque fue una nueva forma de comunicación dentro y fuera de la misma sociedad, las personas son conocidas como usuarios, cuya principal característica, reside en que no tenían por qué encontrarse en la misma ubicación.

El conocimiento sobre internet, y el acceso al mismo por parte de más y más usuarios consiguió, que se reforzará y traspasará fronteras, tanto físicas como idiomáticas, por supuesto también, culturales (este aspecto suele ser más reticente al cambio).

La clave del éxito es, la posibilidad que éstas ofrecen de comunicación entre usuarios de manera inmediata, sin importar, la ubicación de los usuarios, no importa donde esté tu amigo, si tiene internet, puedes comunicarte con él.

La primera red social de la que se tiene constancia es SixDegrees en 1997, pasando por MySpace y LinkedIn en 2003, Facebook en 2004, Twitter 2006, WhatsApp 2009, Instagram 2010, TikTok 2016, y creo que no es conveniente cerrar la lista, porque cada día nos sorprendemos con una aplicación nueva.

En la siguiente imagen contemplamos la línea temporal de las redes sociales.

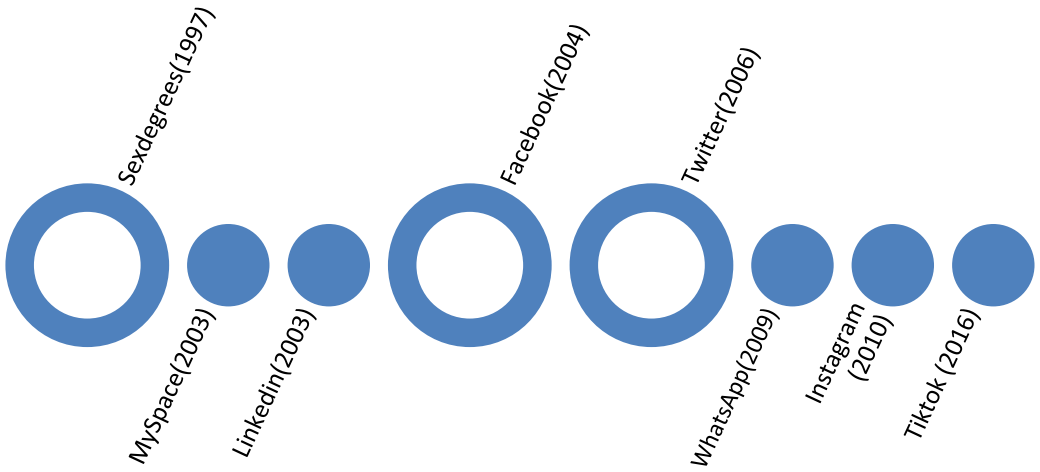


Gráfico 1: evolución de las redes sociales. Elaboración propia. Fuente: marketing4ecommerce.

1.2. Tipos de redes sociales y análisis.

Desde hace más de dos décadas las redes sociales se han convertido en algo presente en nuestras vidas, a pesar de que son muy jóvenes, como he mencionado las redes sociales parten del año 1997, aunque las que más se usan en este momento, por ejemplo, Facebook y WhatsApp, son mucho más recientes, nacen en el año 2004 y 2009 respectivamente.

Son herramientas que nos permiten comunicarnos con el resto de la sociedad, sin importar el lugar donde residan, lo que también hace que se interactúe con mucha más frecuencia. También han provocado que nuestros pensamientos, ideas, etc. hagan partícipe a muchas personas, es decir, lanzamos nuestra idea, y una gran variedad de personas la recogen, provocando multitud de reacciones como feedback positivo y negativo.

Este autor Derek L. Hansen nos muestra en su libro las claves de su análisis.

"Los sistemas de redes sociales se pueden caracterizar por seis dimensiones principales que conforman el marco de diseño de las redes sociales: Tamaño de la población de productores y consumidores; Ritmo de interacción; Género de elementos básicos; Control de elementos básicos; Tipos de conexiones; Retención de contenido. Existen muchos tipos de sistemas de redes sociales que incluyen conversaciones asincrónicas, conversaciones sincrónicas, World Wide Web, autoría colaborativa, blogs y podcasts, intercambio social, servicios de redes sociales, mercados y producción en línea, generación de ideas, mundos virtuales y servicios móviles".[2]

[2] Derek L. Hansen, ... Itai Himelboim, en el análisis de los medios sociales Redes con NodeXL (segunda edición), 2020

A continuación, un pequeño análisis de las redes que más se utilizan por los usuarios, son:

- ***WhatsApp***. Es una de las redes más utilizadas en todo el mundo. Debido a su configuración, simplicidad, multitud de idiomas. Esta app originaria de Estados Unidos tiene 590 millones de usuarios registrados, de los cuales 350 millones son usuarios activos mensuales. Está disponible en 100 países.

- ***Facebook***. Es una red social gratuita creada por Mark Zuckerberg. Permite a cualquier persona con una cuenta de correo contactar con más usuarios de esta misma red, crear perfiles, grupos. Es una de las más aprovechadas por las pymes para publicitarse.

- ***Instagram***. Es una aplicación que permite tomar fotografías y modificarlas con efectos, para luego compartirlas en redes sociales. El uso de esta red, se traduce en subir y publicar imágenes, en los que las personas de tu red y cercanas, pueden indicar que les gusta, y a la vez realizar comentarios de dicha imagen. Es una red social que adquirió Facebook recientemente. Instagram es la red social del momento y es la que mayor crecimiento está teniendo hasta el momento.

- ***Telegram***. Se usa en gran parte del mundo, como sustituta de WhatsApp.

- ***TikTok***. Fundado en mayo de 2017, TikTok es la plataforma líder de vídeos móviles de formato corto (15 segundos mínimos y 60 segundos máximos) creados en dispositivos móviles. TikTok se extiende a todos los mercados principales, con la excepción de China, donde otra app, Byte Dance ofrece una aplicación de vídeos cortos distinta llamada Doujin.

- ***YouTube***. Como red social YouTube permite a todos los usuarios sin obligación de registro, poder consumir videos en cualquier momento y lugar,

mediante una conexión a internet. No importa el dispositivo del que se disponga. Fue creado en 2005 en California.

- ***People***. People es la app para descubrir las mejores recomendaciones de restaurantes, libros, películas, series y mucho más gracias a tus amigos e influencers favoritos.

- ***Twitter***. fusiona el concepto de una red social con la de un blog, lo que se define como microblogging. Su objetivo es tener publicaciones cortas y objetivas que faciliten la transmisión de las informaciones. Ha sido denominado como el "SMS de Internet ".
- ***Tapatalk***. Una aplicación para todos los foros La idea de Tapatalk es sencilla, unificar el uso de los foros que visita asiduamente el usuario para facilitarle la vida ahorrando tiempo, todo desde una única aplicación.

- ***Tinder***. es una red, cuya finalidad, es conectar a personas "desconocidas", que quieren conocer a individuos, principalmente para mantener relaciones íntimas.

- ***Twitch***. Para los amantes del videojuego; es una plataforma web, que usan los "gamers", para partidas jugadas por usuarios para ver jugar a los profesionales de los videojuegos, para escuchar sus comentarios, etc., surgió en junio de 2011

- ***Waze***. es una app, en la comunidad de participa, informa y actualiza información, sobre el estado del tráfico en su ciudad, esto incluye desde calles cortadas, accidentes, controles, etc.; es decir toda la información relacionada con el tráfico en cada localidad

- ***Pinterest***. Sirve para compartir imágenes, ya sean fotos profesionales, books, etc., se usa habitualmente por profesionales fotográficos, y personas que quieren compartir su trabajo.

- ***21 Buttons***. Se dedica al mundo de la moda que te permite obtener ingresos para compartir tus looks. Fundada en 2015 en Barcelona y permite a los influencers, llamados "buttoners", publicar sus looks y recibir una comisión por cada compra generada a través de un sistema de afiliación.

- ***Tumblr***. Tumblr es una plataforma de microblogueo que permite a sus usuarios publicar textos, imágenes, vídeos, enlaces, citas y audio a manera de tumblelog.

- ***LinkedIn***. LinkedIn es una red social cuyo objetivo principal es crear relaciones comerciales y profesionales entre los usuarios

En los siguientes gráficos, proporcionados por el IAB, en los que se muestra una comparativa, sobre gustos en cuanto a redes sociales

Año 2019

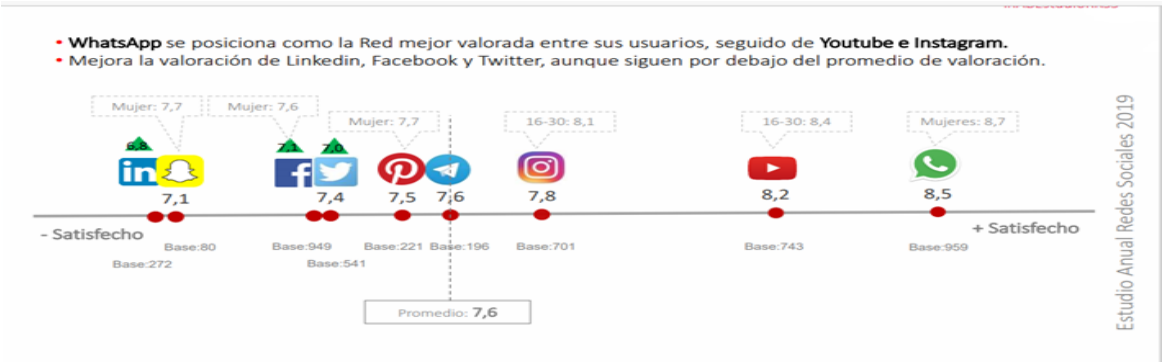


Gráfico 2: Preferencias en uso de redes sociales año 2019. Fuente: Estudio de Redes Sociales, IAB España.

Año 2020

Gráfico 3: Preferencias en uso de redes sociales año 2020. Fuente: Estudio de Redes Sociales, IAB España.

1.3. Datos de uso.

La sociedad en la que vivimos, desde hace unas pocas décadas, ha evolucionado sin precedentes, y desde la pandemia, ha sufrido una pequeña paradoja que paso a describir. Esta paradoja se debe a que no nos hemos podido mover de nuestros hogares, sin embargo, nuestra actividad en las redes sociales no ha tenido comparación con otros momentos medidos y vividos.

En la que la mayoría de los ciudadanos usamos la red; y tenemos la sensación y creemos que el resto de las sociedades que nos rodean, independientemente del nivel de riqueza y de la cultura en la que estén inmersos, tienen una realidad en consonancia con la nuestra.

La idea de que todos tenemos y usamos internet, es debido a que vivimos en un país desarrollado, con libertad, pero debemos ser conscientes de que de los millones de personas que existimos en el planeta, no todos tienen la capacidad de acceder a internet, y tampoco la opción de poder hacerlo.

Existen determinados países en los que tienen prohibidas determinadas páginas web, o simplemente no se implanta la infraestructura para que sus ciudadanos puedan acceder a la red; o puede llegar el caso también de que haya poblaciones inmersas en sus raíces culturales y no quieren pertenecer a este mundo de la red.

Es por este motivo y viendo el tema que nos ocupa desde un prisma diferente, se debe tener en cuenta una serie de indicadores o características fundamentales para entender el grado en que las empresas de todo el mundo puedan darse a conocer en la red.

Paso a resumir los indicadores o características que analizamos, son los siguientes: Disponibilidad, Asequibilidad, Relevancia y Preparación:

El indicador de *disponibilidad*, examina la calidad y la amplitud de la infraestructura disponible requerida para el acceso y los niveles de uso de Internet. Entre las regiones.

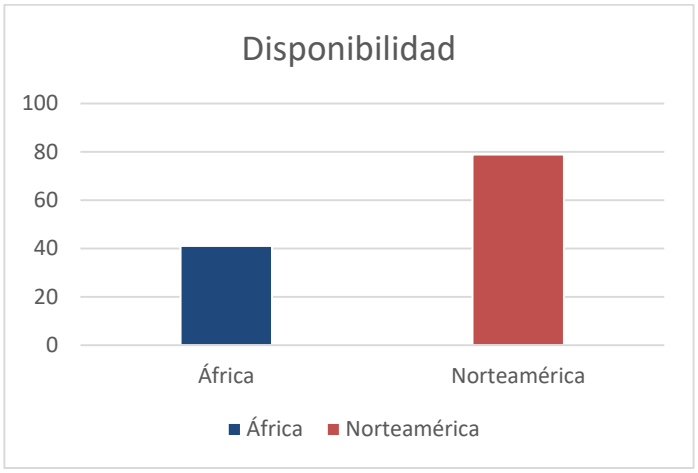


Gráfico 4: Disponibilidad de Red. Elaboración propia. Fuente: ONSTI.

El siguiente factor que tenemos en cuenta es la *asequibilidad*, se podría definir como el coste que implica la infraestructura, en relación con la renta y el nivel de competencia del mercado.

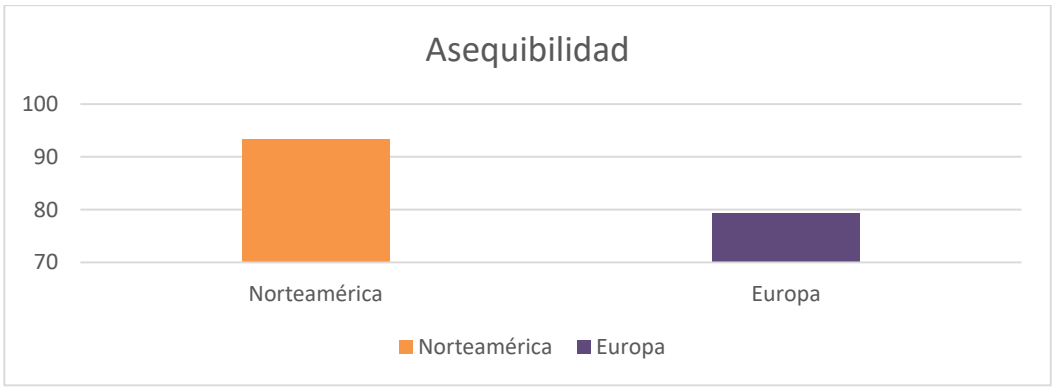


Gráfico 5: Asequibilidad para red. Elaboración propia. Fuente: ONTSI

En tercer lugar, se encuentra la *relevancia*, este indicador se refiere al alcance que los contenidos tienen a nivel mundial, teniendo en cuenta otras dos circunstancias, el idioma que puede ser un obstáculo o un punto a favor, y el contenido, la información que se quiere publicar.

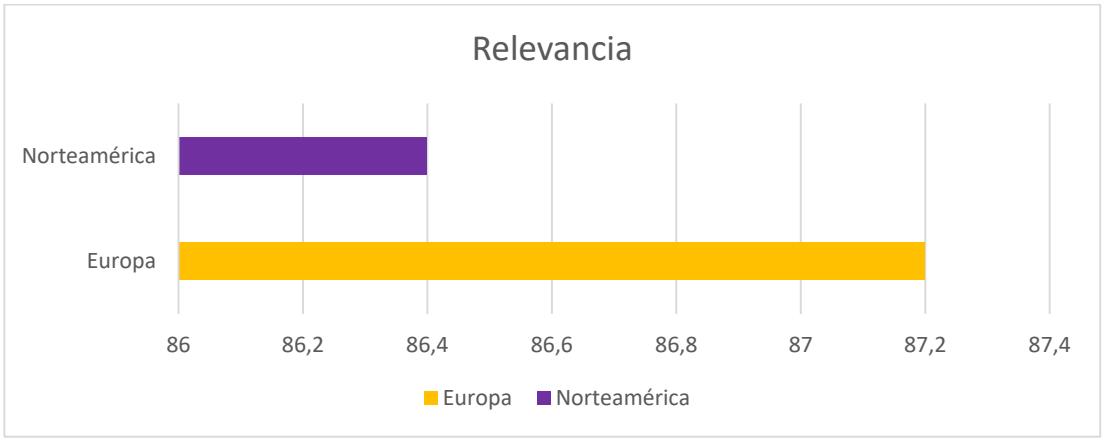


Gráfico 6: Relevancia en difusión de información. Elaboración propia. Fuente de datos: ONTSI.

La *preparación* es el indicador que mide y valora la capacidad de la población y de sus gobiernos de tener una actitud cultural positiva y de adaptación hacia internet, mediante la formación y el acceso a herramientas que lo faciliten.

El estudio que realiza el ONTSI, recoge los datos de las pymes españolas y las europeas, en el siguiente gráfico se muestra la media con respecto a la cobertura o acceso a internet.

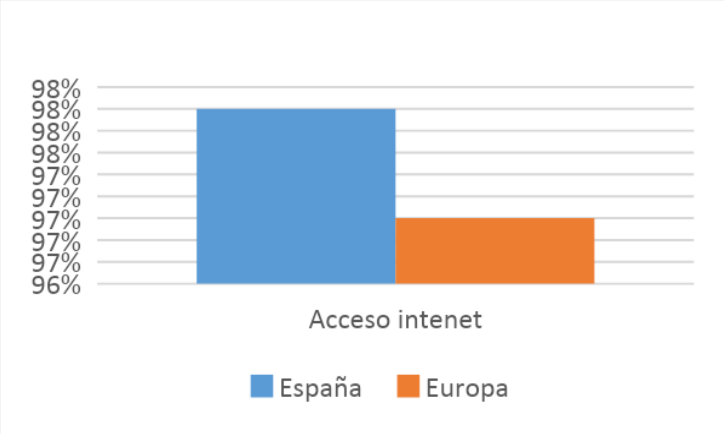


Gráfico 7: Cobertura. Elaboración propia. Fuente: ONTSI

La cobertura puede parecer un dato menor, pero desvela la disponibilidad, como he mencionado el grado de infraestructura, que es uno de los factores fundamentales para el acceso a internet, de todo tipo de consumidores, particulares, administración y empresas.

Aun siendo España un país, no avanzado respecto al resto de países de la Unión Europea, la cobertura actual de internet, supera a la media. Encontrándose justo por debajo de los 10 primeros países, con mayor cobertura de producto.

1.4. ONTSI.

El ONTSI[3] es el Observatorio Nacional de Tecnología y Sociedad, siendo el objeto crear informes sobre el impacto de la tecnología en los distintos ámbitos de la sociedad, tales como servicios públicos, seguridad, calidad de vida, etc. Es una entidad público empresarial, cuyo estatuto, se definió a través del Real Decreto 164/2002.

El observatorio realiza informes, en los que muestra los indicadores, relacionados con políticas y estrategias, evalúa programas, también tendencias de la sociedad, identifica buenas y malas prácticas, y publica la información para que pueda llegar al máximo número de personas posible. El objetivo fundamental, al crear los informes, es ser un referente de información sobre análisis y seguimiento de la Sociedad de la Información en España.

Para poder ser fiable, solicita información tanto en el sector público como en el privado, para que ésta se lo mas completa posible. A continuación, contrasta la información y los datos obtenidos.

El ONTSI, como todo ente tiene unos estatutos en los que define de forma tasada, las funciones que debe desarrollar, y en el artículo 21.1 de los Estatutos de la Entidad red.es señala, como ejemplo:

- Seguimiento y estudio de la política desarrollada por la Administración, en el ámbito de las telecomunicaciones y de la sociedad de la Información, así como la evolución de las mismas, con objeto de mejorar y ampliar su marco referencial.
- Valorar el desarrollo y la evolución de las telecomunicaciones y de la sociedad de la información en el ámbito empresarial, en especial en las

[3] Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (2020). La sociedad en red: Transformación digital en España: Informe anual 2019. Madrid: Secretaría General Técnica, Centro de Publicaciones

pequeñas y medianas empresas, y elaborar un informe anual sobre los mismos, para lo que se dispondrá de la información estadística necesaria.

La ONTSI centra su estudio y evaluación de los informes en tres áreas: indicadores, estudios y políticas públicas.[4]

Con respecto a la primera, ***los indicadores***. Crear, recopilar y coordinar fuentes de información (nacional e internacional) sobre la Sociedad de la Información. Los indicadores analizados por el observatorio, son conectividad, capital humano, uso de Internet, integración de la tecnología digital y servicios públicos digitales.

Con respecto al área de ***estudios***. Ésta es la encargada de la realización de las investigaciones que analizan el desarrollo de la Sociedad de la Información y la transformación digital en España, en el ámbito de los hogares y ciudadanos, empresas y en el sector de las Tecnologías de la Información y las Comunicaciones.

Por último, ***las políticas públicas***. Analiza las políticas y las diferentes estrategias digitales tanto nacionales como internacionales.

Los informes que realiza el ONTSI, son análisis detallados de la información más importante que muestran los indicadores y áreas. No es un enfoque mono focal, sino una visión global, a nivel mundial y europeo, que posibilita contextualizar y comparar los resultados españoles con el resto de los países, permitiendo así obtener una visión objetiva y lo más completa posible de la situación actual.

El análisis y posterior informe, plasma la información recabada desde tres perspectivas, el sector empresarial, la ciudadanía y la Administración pública, lo que

[4] Observatorio Nacional de Tecnología y la Sociedad (2021). Indicadores de uso de Inteligencia Artificial en las empresas españolas. Madrid: Ministerio de Asuntos Económicos y Transformación Digital, Secretaria General Técnica. https://www.ontsi.red.es/es/dossier-de-indicadores-pdf/indicadores-uso-inteligenciaartificialempresas-espanolas

permite de una manera práctica y muy eficaz observar el grado de uso e impacto que pueden tener las diferentes soluciones tecnológicas en los diferentes ámbitos.

1.5. Campos y sectores en los que las redes sociales tienen influencia.

Las redes sociales están adquiriendo mucha fuerza en muchos ámbitos de la vida, entre ellos, destacan: el e-commerce, publicidad, el marketing, los recursos humanos, la forma de trabajar, las plataformas educativas, periodismo etc.

Uno de éstos es el de *selección de personal.* Las propias empresas, o personal profesional dedicado de forma exclusiva a este fin, cuya función es buscar información a través de internet y las redes sociales, sobre gustos, aficiones, preferencias ideológicas, de los candidatos que quieren acceder a puestos ofertados por las empresas.

Buscan por todas las redes posibles, todo tipo de información que pueda ser útil, para obtener un perfil mucho más detallado, del que se aporta en un cv.

En cuanto al *e-commerce*, las redes sociales se han convertido en una de las mayores ventanas de publicidad para todo tipo de empresas que podían ser pequeñas y sobrevivían con el comercio a pequeña escala, o simplemente el presupuesto para estas partidas era tan reducido que ni siquiera se lo planteaban.

De esta forma, se han abierto al mundo, debido a que crear una página web, no tiene un coste alto, y crear un perfil de la empresa en redes sociales es gratuito. Por lo que se ha hecho muy fácil llegar a un mayor público, de forma mucho más sencilla y barata.

Por otra parte, lo bueno de las redes sociales es que son globales, por lo que, aunque residas en una ciudad “perdida” tu producto se puede ver en cualquier parte del mundo.

Otro sector importante, que ha evidenciado el fuerte crecimiento de las redes sociales es la *publicad y el marketing*. Ha experimentado un boom.

Es el marco perfecto para experimentar toda estrategia de marketing y publicidad, obteniendo resultados rápidos. Otro de los puntos positivos radica en el coste que conlleva, se reduce de manera considerable.

Permite variedad de opciones, como cuñas de YouTube, encuestas, mini videos promocionales, etc.

En cuanto a las *plataformas educativas*, se puede asegurar que han tenido un boom, como el que comentábamos del marketing.

Cierto es que hay un gran número de centros de enseñanza que tenían modalidad online, y a pesar de ello, han reforzado y actualizado su estructura para una mejor cobertura de cara al empleado y alumnado.

A parte de las instituciones que ya tenían implantado este sistema; gran parte del ámbito educativo a nivel nacional e internacional han experimentado este gran cambio, de forma voluntaria y obligatoria.

Sobre todo, en este momento de confinamiento y pandemia, escuelas, universidades, academias, etc. Se han tenido que readaptar al sistema de dar clases online, a través de aplicaciones como Skype, Zoom; o crear plataformas propias como la Uva.

O como el ejemplo de universidades estadounidenses, que aprovechando la coyuntura y ante la gran demanda de cursos ofertados, han creado Mooc´s para impartir cursos para que puedan ser vistos por toda aquella persona con interés.

Gestión de recursos humanos e investigación de empleados. Como mencionaba anteriormente las propias empresas, o personal profesional dedicado de forma exclusiva a este fin, cuya función es buscar información a través de internet y las propias redes sociales, sobre gustos, aficiones y preferencias ideológicas, de los candidatos.

Publicidad, comunicación, estudio de mercados. Es el marco perfecto para experimentar toda estrategia de marketing y publicidad, obteniendo resultados rápidos.

2. USO DE LAS REDES SOCIALES EN LA COMUNICACIÓN LABORAL Y EMPRESARIAL. REDES SOCIALES Y MENSAJERÍA.

2.1. Comunicación interna en las empresas, y teletrabajo

Como es sabido uno de los pilares fundamentales de las empresas, es la comunicación interna, esto se produce en las empresas tanto si disponen o no de gran cantidad de empleados. Hasta hace poco tiempo, para llevarla a cabo se realizaba de forma presencial principalmente haciendo reuniones de equipo, y también haciendo llegar a los empleados circulares, etc.

En la actualidad la forma de hacer llegar a los empleados la información relevante de la empresa, ha cambiado en gran medida. Por una parte, se realiza a través de la intranet de la empresa o por correo electrónico corporativo; y, por otro lado, normalmente se publica a través de las redes sociales.

Según comentaba en el capítulo primero, son varias las aplicaciones que se utilizan para la comunicación interna de las empresas. El uso de las redes sociales para esta comunicación interna se puede deber a varios motivos, entre ellos tenemos como uno de los más importantes, no tener la tecnología adecuada dentro de la propia empresa; por otra parte, importante reseñar que no se disponga del coste que implica instalar el soporte adecuado.

La comunicación interna también evoluciona debido a que como he comentado en sectores donde se han implantado el teletrabajo, como búsqueda de talento fuera de una zona geográfica concreta; también hemos cambiado hábitos y maneras de trabajar porque la pandemia que estamos atravesando nos obliga, adaptándonos todos a la *"nueva normalidad"*. Esta nueva normalidad, como solemos escuchar habitualmente,

"ha llegado para quedarse", por este mismo motivo son muchas las empresas que están adaptando su estructura y forma de trabajo a esta nueva modalidad.

La adaptación en algunas empresas ha supuesto un gran esfuerzo, en otro prácticamente ninguno. Las ventajas con las que cuenta el teletrabajo son ahorro de costes fijos en la empresa; y teniendo como inconvenientes del teletrabajo la implantación de medios de seguridad para llevarlo a cabo, imposibilidad de desconexión del trabajo, etc.

2.2 Comunicación externa.

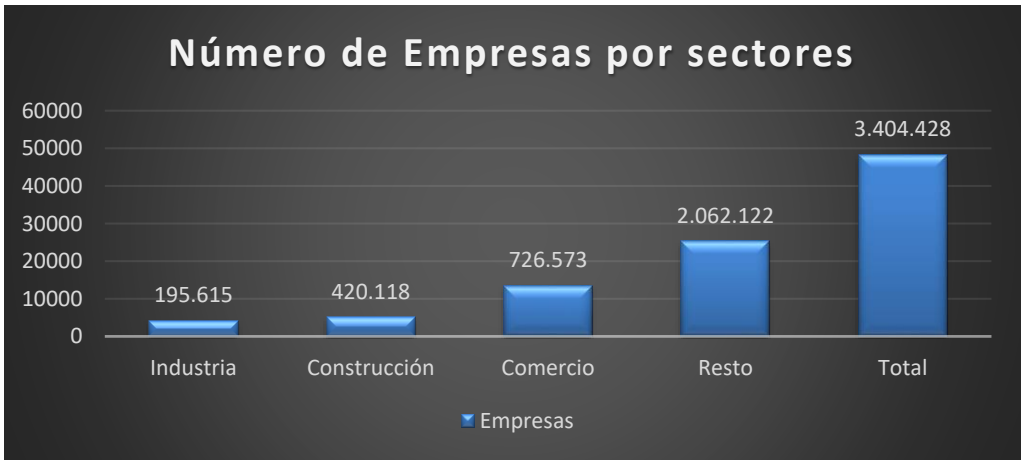


Gráfico 8: Número de empresas por sectores. Elaboración propia. Fuente:.INE.

Entendemos por comunicación externa de una pyme, la forma en que se comunica ésta con su entorno. Para llevarla a cabo actualmente se realiza de varias formas, las más importantes son a través de una web corporativa y mediante un perfil en redes sociales.

El siguiente gráfico muestra una comparativa, de las empresas que poseen una web corporativa, y las empresas que usan redes sociales.

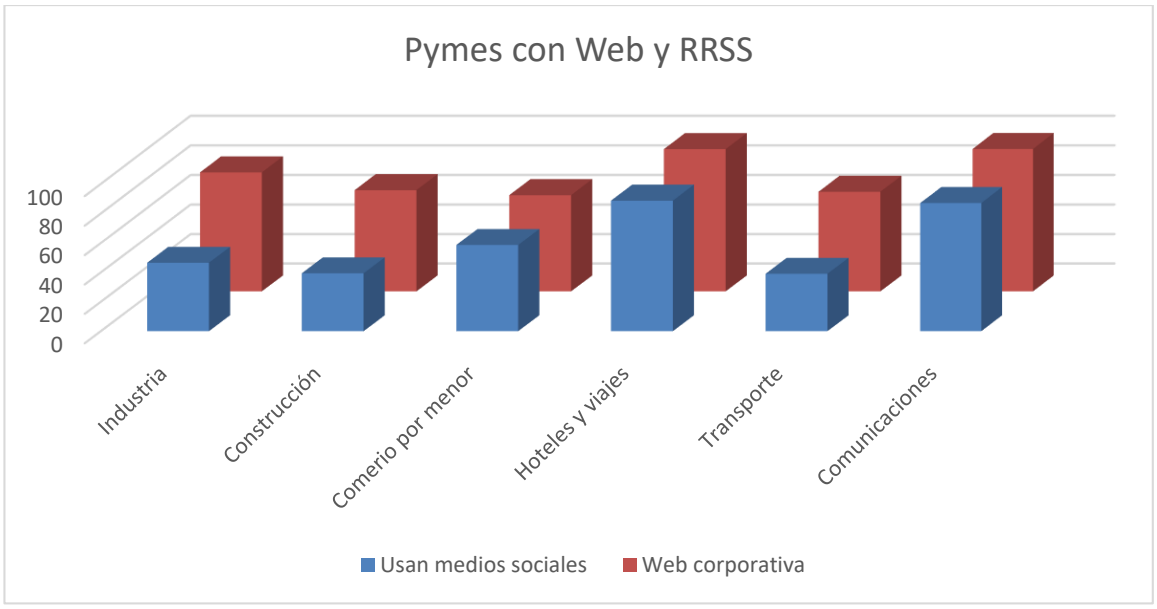


Gráfico 9: Pymes con web corporativa y uso de redes sociales. Elaboración propia. Fuente: ONTSI.

En el gráfico se muestra las pymes que poseen web corporativa y, además, tienen perfiles en redes sociales, para darse a conocer, en un espacio hasta hace poco desconocido. Lo habitual en este caso, es como punto de partida tener en el equipo a un profesional que sepa, por una parte, gestionar las redes sociales de forma correcta, y, por otra parte, que tenga conocimientos legales, para mantener a la empresa que representa siempre en la legalidad, con respecto a las publicaciones y publicidad que realice.

Año	2012	2016	2020
España	6	12	12
Europa	7	8	7
	85%	150%	171%

Tabla 1: profesionales contratados para gestionar redes sociales. Fuente: elaboración propia.

2.3 Tendencias y cambios.

Desde sus inicios, el ritmo de los avances de la red e internet evoluciona de forma vertiginosa, y dentro de éstos se crean, modifican y eliminan elementos de internet, a medida que la red madura.

Como hemos visto internet surgió como un instrumento útil y exclusivo para un fin determinado en tiempos de guerra en los años 50; ha evolucionado, y con el paso de los años, se ha extendido de forma exponencial hasta nuestros días. Se ha producido la evolución y su expansión en todos los ámbitos de la vida, y de acuerdo a esa evolución y las exigencias de la sociedad, se amplía la gama de servicios, funcionalidades y herramientas que se crean, modifican y suprimen, a nuestra disposición. Y esto se debe a que las funcionalidades a nivel usuario, pueden llegar a ser casi infinitas, y su uso sea inferior al deseado puesto que en realidad conocemos muy pocas aplicaciones en comparación con las que existen.

Podemos observar funcionalidades y aplicaciones de internet para todos los niveles, son las tendencias las que convivimos, y las que se presentarán a corto plazo. Las denominamos tendencias de la red, para situarnos, haré una breve indicación de las funcionalidades. Algunas de ellas son conocidas, y otras se implantarán en breve:

- Los audios online; asistentes virtuales, streaming. Estas nuevas aplicaciones aparecen en torno a 2019, y se integran de manera veloz en nuestros hogares y empresas en 2020. la característica fundamental es la voz, que es una forma muy sencilla y cómoda de comunicación, se adapta al estado de ánimo del usuario.
- Branded Content; contenidos interactivos, fake news, podcast. Una de las nuevas tendencias que se producía ya en 2019, son las fake news, se usa como técnica de desinformación cada vez más sofisticada, y sobre todo en el área de la política, por ello desde la Unión Europa se esperan las primeras regulaciones en la materia. Viendo el cariz que las fake news alcanzan, las plataformas en línea y demás áreas comprometidas en la información en red,

han desarrollado y adaptado un Código de buenas prácticas contra la desinformación.

- E-Commerce; webs comparadoras, tv commerce. marketplace. Las webs comparadoras siguen en alza, y como consecuencia se expanden abriendo sus mercados a otros sectores diferentes de seguros y compañías.
- Pago a través de redes sociales. De momento, solo ciertas redes ofrecen la opción de pagar mediante su plataforma, que hace que se normalice el social shopping, desde su plataforma.
- Influencers; inteligencia artificial. La inteligencia artificial será fundamental, porque se creará mediante algoritmos exclusivos para cada marca. Esto permite organizar y dar más valor a los datos contenidos; y por supuesto permite automatizar procesos. Este sistema es muy útil en el sector publicitario, por la optimización de campañas y recursos, que equivale a tomar mejores decisiones y a su vez mejores estrategias.
- Redes sociales; personal y local, usuarios exigentes, generación z. La generación Z se refiere, a la población más joven, son usuarios cada vez más exigentes en nuevas tecnologías y los que marcan las tendencias en redes sociales, debido a que son los que más las usan.
- Vídeos online; formatos y duraciones, realidad aumentada. Como indicaba, esto es solo una breve referencia de la aplicación, que disponemos a nivel de usuario.

Además de las aplicaciones analizadas incorporo una sucinta mención a varias aplicaciones más, debido a que el listado es extenso.

- Branding; animaciones de marca, mindful marketing, relatos.
- Data; el 5G, inteligencia artificial, gestión de identidad.
- Digital out of home; interactividad, formatos impulso a la compra programática.
- Directiva audiovisual.
- Cookies y e-privacy; datos personales como contraprestación.

- E-sports; las nuevas plataformas.
- Innovación tecnológica; 5G, altavoces inteligentes.
- Mobile; app, híper personalización.
- Programática; Smart tv, supply chain.
- Los supply chain son protocolos técnicos que ayudan en cuanto a transparencia y seguridad, y permiten la trazabilidad en compra de publicidad.
- Cómo hacer video marketing en directo: Twitch, TikTok e Instagram
- Cómo mejorar la customer experience, con fitness Digital, y Opiniones Verificadas
- TCPF, la propuesta con la que IAB Spain quiere liderar la nueva era post-cookies
- 4 consejos para sacar el máximo partido a los eventos híbridos de networking profesional
- Empresa lanza un videojuego en Facebook e Instagram para conquistar a los usuarios más jóvenes
- Cómo utilizar Instagram para ayudar a tu eCommerce
- Y, en este sentido, no solo hablamos del mundo laboral, donde el teletrabajo, las herramientas colaborativas o las videoconferencias han sido los absolutos protagonistas del año, sino también del mundo personal, ya que muchos de nosotros ya nos hemos pasado al canal online de nuestro supermercado de confianza, a hacer video llamadas grupales con amigos o a, ahora que por fin tenemos más tiempo, formarnos en aquello que siempre nos había apasionado, como podría ser, por ejemplo, las últimas innovaciones y tendencias del entorno digital.
- Entregas same day y su eficacia al fidelizar a los clientes
- Google refuerza su apuesta por el eCommerce: alianza con Shopify, nuevo Shopping Graph y productos en Google Lens.

En otra sección de aplicaciones, también tenemos tendencias en cuanto a la medición de impacto de las empresas que se posicionan en las redes sociales más usadas para desarrollar sus negocios:

Facebook Insights [5] es una de las mejores herramientas para poder extraer los datos examinados de tu página de Facebook. Es una herramienta muy valorada, la que más suelen utilizar dado que es gratuita y te permite extraer mucha información.

Las funcionalidades de esta herramienta son muy prácticas e intuitivas. ya que se puede realizar el seguimiento, siendo un usuario común, o como usuario profesional.

Para ir a las estadísticas de Facebook Insight, debes entrar a Fan Page, se puede realizar de dos maneras:

1. Entrando directamente**.** Seleccionando el acceso directo a la página de Facebook. Esta opción sirve para gestionar las páginas sin abandonar tu perfil de usuario e interaccionar con tus contactos.

2. Business Manager**.** Una vez estés dentro, en el menú ubicado entre la franja azul situada arriba y la imagen de portada, encontrarás la pestaña de Estadísticas ubicada entre Notificaciones y Herramientas de publicación.

Las opciones de notificaciones son variadas, y para el día a día de la empresa, es muy versátil, por sus posibilidades que se actualizan constantemente.

La web de Facebook Insight nos ofrece una guía y una lista, de beneficios que podemos obtener con su uso:

Hay 9 recuadros con las siguientes métricas:

• Acciones en la página. Número de clics en la información de contacto de tu página y el botón de llamada a la acción.

• Visitas a la página. Número de veces que los usuarios que han iniciado sesión y no han iniciado sesión han visto el perfil de una página.

---

[5]Información sobre Facebook Insight https://www.publicidadenlanube.es/facebook-insights-tutorial-espanol/

• Vistas previas de página. Número de veces que los usuarios han pasado el cursor por el nombre o la foto del perfil de la página para obtener una vista previa de su contenido.

• *"Me gusta"* de la página. El total que tiene y el número de *"Me gusta"* de esta semana, junto con un porcentaje en comparación de los resultados obtenidos la semana pasada. Si es inferior se muestra en rojo y con un indicativo negativo, si la comparación es superior se muestra en verde y con el indicativo positivo.

• Alcance de la publicación. El alcance total y el alcance de la publicación (esta diferencia la explicaré más adelante) de la última semana junto con los porcentajes comparativos.

• Recomendaciones. Las veces que han recomendado tu página.

• Interacción con la publicación: Número de veces que los usuarios han interactuado con tus publicaciones al indicar que les gustan, comentarios, compartirlas, etc.

• Vídeos. La cantidad de veces que se reprodujeron los videos en tu página durante al menos 3 segundos, o durante casi su duración total si son menores de 3 segundos, desglosados por total, pago y sin pago. Durante una única reproducción de video, excluyendo el tiempo dedicado a reproducir el video.

• Seguidores de la página. El número de nuevos seguidores.

2.4. INCIBE[6]

Instituto Nacional de Ciberseguridad.

[6] INCIBE https://www.incibe.es/que-es-incibe

INCIBE es el instituto oficial estatal, cuyo objetivo principal es tratar de crear y asentar la seguridad digital en la sociedad. Para asentar esa confianza en todos nosotros, desarrollaremos acciones en temas de ciberseguridad sobre todo en el espacio de mercados digitales, que son en los que nos solemos encontrar más vulnerables, e impulsar la confianza en este medio, en nuestro país.

El Incibe, instituto Nacional de Ciberseguridad, en sus orígenes fue nombrado anteriormente Instituto Nacional de Tecnologías de la Comunicación.

Incibe actualmente depende o cuelga del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

Esta sociedad se ha consolidado como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

Desde sus inicios está inmersa en la permanente búsqueda e investigación de servicios, para proporcionar ciberseguridad. a su vez se coordina con agentes e instituciones con competencias en la materia.

MISIÓN

La misión de **INCIBE** es por tanto reforzar la ciberseguridad, la confianza y la protección de la información y privacidad en los servicios de la Sociedad de la Información, aportando valor a ciudadanos, empresas, Administración, red académica y de investigación española, sector de las tecnologías de la información y las comunicaciones y sectores estratégicos en general.

VISIÓN

La visión de **INCIBE** es conseguir sus objetivos mediante:

1. El compromiso de profesionales altamente cualificados, comprometidos con sus proyectos y capaces de generar valor e innovación de forma continua.

2. La dinamización del sector TIC, desde una perspectiva de igualdad de oportunidades, generando nuevos negocios y oportunidades para clientes, proveedores y profesionales.

3. El soporte a los ciudadanos, empresas, administraciones, Red Iris junto con sus instituciones afiliadas y sectores estratégicos, todos ellos claves para un desarrollo de las nuevas tecnologías con un alto impacto social.

4. La generación de inteligencia en ciberseguridad como medio necesario para el desarrollo de tecnologías y conocimiento a aplicar en nuevas herramientas y estrategias.

VALORES

Los valores que promueve **INCIBE** son los siguientes:

- Transparencia con la sociedad en general y los agentes del ámbito de la ciberseguridad en particular.
- Búsqueda de la excelencia, tanto en la aptitud y en la actitud de sus profesionales, así como en la ejecución de los proyectos.
- Vocación de servicio público.
- Mantenimiento del espíritu innovador y de la búsqueda de la excelencia en los proyectos que se abordan, maximizando el valor ofrecido.
- Sostenibilidad como valor ético y criterio de desempeño que involucra los aspectos económicos, sociales y medioambientales de la actividad.
- Espíritu de integración, apoyo y cooperación con todos los agentes relevantes en ciberseguridad, reforzando las capacidades nacionales en seguridad.

RECOMENDACIONES DE INCIBE PARA EMPRESAS POR SECTOR

INCIBE en su página web ofrece y posibilita, la descarga de aplicaciones para la protección de las webs corporativas

Turismo y ocio.

Hoteles, gimnasios, restaurantes, locales de ocio, agencias de viajes… El sector servicios, debido a su actividad laboral, gestiona una gran cantidad de información personal de los clientes, así como las reservas y horarios elegidos.

Puesto que los **datos personales de los clientes son vitales para cualquier empresa**, ya que de ellos depende el correcto funcionamiento de la misma, ante un incidente en el que se vieran involucrados la compañía podría sufrir graves consecuencias legales o que afecten a su continuidad o a la confianza de los clientes.

Logística.

Empresas de almacenamiento y explotación de infraestructuras para el transporte, actividades postales, transporte y distribución de productos o pasajeros, etc. Las compañías de este sector utilizan diferentes tecnologías como las apps para dispositivos móviles, escaneo de documentos, plataformas online, herramientas de *tracking* (seguimiento de paquetes), etc., imprescindibles para que la actividad diaria no se detenga. También gestionan información personal de clientes, que debe estar protegida adecuadamente para evitar fugas de información que puedan afectar a los usuarios y a la empresa.

Comercio minorista.

Bazares, quioscos, papelerías, tiendas de ultramarinos, fruterías o zapaterías son solo algunos ejemplos de comercios minoristas. Estas empresas, en su mayoría micro pymes y autónomos, son además objetivos fáciles de atacar por los ciberdelincuentes. Cuando una empresa de este sector sufre un fraude, una infección por *malware* u otro incidente de seguridad, las consecuencias pueden suponer el fin para el negocio.

Salud.

Clínicas de todo tipo, especialistas sanitarios, personal de enfermería y obstetricia, laboratorios o farmacias son algunos ejemplos de empresas de este sector.

El personal de estas empresas es muy variado, pero tiene en común que, de una manera u otra, gestiona información muy sensible, siendo la privacidad y disponibilidad de esta información factores clave para su negocio.

Comercio mayorista.

Venta o distribución de productos al por mayor en alimentación, electrónica, textil, etc. son algunos ejemplos de actividades incluidas en el sector del comercio mayorista, formado en gran parte por pymes con media o alta dependencia tecnológica, entre otras cosas, con página o tienda web, uso cotidiano del correo electrónico, empleo de sistemas ERP (*Enterprise Resource Planning*) y presencia en las redes sociales. Esto os hace estar en el punto de mira de los ciberdelincuentes sobre todo si no contáis con medidas y políticas de seguridad. Cuando sufrís un ciberataque las consecuencias pueden llegar a parar la actividad y afectar muy negativamente a vuestro negocio.

Educación.

El sector de la educación engloba todo tipo de organizaciones que se dedican a la enseñanza o a actividades culturales y deportivas, como centros educativos o academias. La implantación de las nuevas tecnologías es importante en este tipo de instituciones y empresas, tanto para su actividad didáctica y sus procesos internos como para la comunicación con otros centros, alumnos, profesores, etc. Además, se hace un uso intensivo de equipos informáticos y redes cableadas e inalámbricas. Por último, cabe resaltar que, en estas organizaciones, por su propia actividad, se tratan datos de las personas que se matriculan para aprender, y en ocasiones estos datos pueden ser de los especialmente protegidos, como es el caso de los datos de menores o de salud.

El consejo que proporciona INCIBE para todos los sectores de la economía en nuestro país que trabajen a través de la red, son:

Lo que no se mide no se puede mejorar. El primer paso que debes dar para proteger la organización es **identificar los riesgos** a los que está expuesto. Seguramente seas consciente de gran parte de ellos, pero quizá existen otros que no

conozcas y que, en caso de materializarse, pondrían en graves aprietos a tu empresa y tus pacientes.

Para ayudar a evaluar los riesgos a los que se enfrenta tu organización, recomendamos utilizar nuestra Herramienta de Autodiagnóstico. A través de una serie de preguntas, esta herramienta le guiará para que pueda determinar cómo es el estado actual de ciberseguridad en su negocio, qué riesgos lo amenazan y qué aspectos debe mejorar.

3. METODOLOGIA E INVESTIGACION

3.1 Fundamento de la investigación.

En vista de lo acontecido desde el año 2019, e inmersos en una catástrofe sanitaria que ha afectado a todos los países del planeta, paralizando la actividad económica como en pocas ocasiones se ha contemplado, y cuyo único medio de comunicación era internet y las redes sociales. Planteo en el siguiente apartado, la oportunidad de realizar un estudio sobre cómo influyen internet y las redes sociales en la vida de las empresas, para ello creo acertado confeccionar un cuestionario de investigación y opinión, en el que se insta a profesionales para que me hagan una valoración de lo que para ellos supone trabajar en ese medio.

El planteamiento es sencillo, se fundamenta en que la sociedad avanza de forma trepidante, y no lo hace sola; sino que es empujada y guiada a través de un nuevo instrumento, desconocido y adictivo, llamado Redes Sociales.

Es sabido y estudiado que en todos los sectores que forman parte del tejido económico, social y político de nuestra sociedad, es afectado directa e indirectamente por este fenómeno.

Por lo que se observa creído necesario y conveniente, hacer partícipe de las opiniones que genera este fenómeno en los diferentes sectores que componen la economía de nuestra sociedad. Para obtener las opiniones deseadas, el instrumento más rápido y eficaz al alcance es un cuestionario.

El mencionado cuestionario, es un instrumento de investigación, que se utiliza habitualmente en el campo de la investigación cualitativa.

En este apartado y para llevar a cabo la investigación del estudio, pide inclinarse hacia una simulación de cuestionario, para recabar información, y no con el objetivo de parametrizar datos. Esto implica que no será un cuestionario al uso, sino uno más particular, centrándose en opiniones y no datos cuantificables; pero como es comprensible de toda pregunta se pueden sacar datos, que se revelarán después en el apartado de las conclusiones.

Se realiza de esta forma, porque se debe ser consciente de que hay numerosos estudios, mucho más metodológicos, mejor estructurados, más sistemáticos, acerca de este tema tan amplio y desconocido a la vez.

Se han realizado varias encuestas, donde se observa el número de personas que usan redes sociales a diario, por sector, por franja horaria, por aplicación, por edad, etc.

Sabedores de todos esos esfuerzos de profesionales en la materia, el objetivo de esta investigación es muy diferente y a su vez no es menos interesante, para el objeto que lleva a realizarlo.

La metodología es sencilla, debido a que no se trata de cuantificar resultados, sino de que un determinado número de profesionales de diferentes áreas, expresen su opinión acerca de lo que supone y pueda afectar en su forma de sustento, trabajar con redes sociales.

También es interesante la opinión de estos profesionales, desde el punto de vista, de la necesidad de todos ellos, de requerir el uso de las mismas, con entusiasmo o no, de su uso.

Para realizar un cuestionario, se deben tener en cuenta las siguientes características, y seguir una estructura determinada.[7]

Las características del cuestionario que vamos a realizar son las siguientes:

Se puede diseñar de diferentes maneras; de acuerdo con el tipo de información que se quiera obtener:

- Tipos de pregunta: opción múltiple, verdadero/falso, etc. En el caso del cuestionario que se realiza la opción es responder de forma redactada, sin límite de espacio, serán de respuesta corta o de párrafo; a elección del encuestado.

- Definición del tiempo del encuestado:

Es interesante definir el tiempo para su realización, no debe ser muy corto, para que se pueda realizar sin atropellos, no muy largo, porque puede incluso quedar en el olvido su realización.

- Se conoce como entrevista estructurada:

Comprende una cantidad determinada de preguntas con respecto a una variable determinada, que es la que se pretende medir.

Se podría catalogar como una entrevista, porque es una forma de conocer el pensamiento de los entrevistados, sobre un tema determinado.

- Las preguntas se pueden organizar por categorías.

Con esta organización, se puede diseñar un cuestionario en el que en primer lugar se redactan las preguntas, y después se pueden organizar de acuerdo a determinadas categorías, que serán filtradas para obtener las respuestas buscadas.

[7] http://cefire.edu.gva.es/file.php/1/moodle/T3_MInteractivos/42_crear_un_cuestionario.html

En el caso de este cuestionario no es necesario, debido a que los sectores profesionales son muy diversos, con opiniones muy diversas.[8]

- Pueden crearse cuestionarios multimedia.

Un cuestionario multimedia, tiene la característica, de que es más entretenido de responder, suele atraer y llamar más la atención; por lo que es aconsejable para determinados ámbitos y grupos de edad.

- Diseño de preguntas por categorías.

Este diseño implica hacer un número indeterminado de preguntas, para después concretar en las que realmente serán útiles para obtener la información deseada.

- Podemos permitir a las personas realizar intentos repetidos sobre una pregunta o bien que respondan el cuestionario varias veces (con la opción de que cada intento se construya sobre el anterior).

- Un cuestionario por sesiones o etapas

Se suelen usar en investigaciones de producto, de concepto, en estudios de mercado, etc.; se usan principalmente para conocer la opinión y grado de aceptación de un concepto e idea.

Realizándose encuestas en varias sesiones, para de esta manera obtener resultados del antes y después.

En el siguiente apartado se muestra el ejemplo del cuestionario que he facilitado a los participantes del estudio. Los resultados del mismo se adjuntan en el Anexo I.

3.2. Cuestionario

Desde el punto de vista de la empresa

[8] Características de los cuestionarios: https://tuescuelita.com/caracteristicas-de-los-cuestionarios/

1. Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa
2. Cuáles cree que son los principales riesgos
3. Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa

    3.1 Comunicación interna

    3.2 Comunicación externa

    3.3 Publicidad

    3.4 Gestión de compras y ventas

4. Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones

Desde el punto de vista de los trabajadores

1. Cuáles son en su opinión las principales oportunidades que aportan las redes sociales en relación a la manera en que los ciudadanos se relacionan con su empleo y su contexto laboral.
2. Cuáles cree que son los principales riesgos
3. Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de los trabajadores

    3.1 Búsqueda de empleo

    3.2 Comunicación con compañeros/as

    3.3 Comunicación con la empresa

    3.4 Gestión de su trabajo

4. Qué consejos daría a un trabajador para gestionar de manera adecuada sus comunicaciones y redes sociales

4. RESULTADOS

El cuestionario efectuado, se centra en 3 focos fundamentales: las redes sociales, el empresario y por último el trabajador.

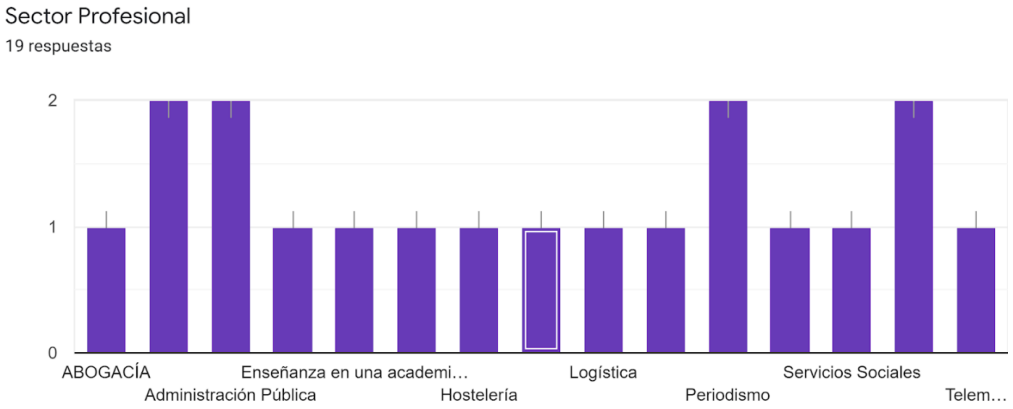
El objetivo principal que se persigue desde el comienzo de este estudio, posterior análisis, seguimiento, y como punto finalizador, obtener resultados reales; sobre la influencia de las redes sociales, y su uso en la vida diaria. Teniendo presente el uso real de las mismas que se produce tanto en la vida social como profesional.

En este caso el estudio de este trabajo se centra en este momento, de forma más específica en el mundo laboral.

Dentro de la metodología, para llevar a cabo el análisis de campo, se establecen 2 cuestionarios; uno de ellos destinado a la persona encargada de gestionar una empresa, negocio, etc. y otro cuestionario destinado al empleado.

Las preguntas del cuestionario, en un primer momento, son iguales o similares; a medida que avanza el cuestionario, divergen debido a que el ámbito de actuación es diferente, hay una jerarquía y unas funciones que varían.

Como se muestra a continuación en el gráfico, para llevar a cabo la investigación, he seleccionado a un número muy reducido de personas, que desarrollan su actividad profesional en diferentes sectores:



Las personas encuestadas son profesionales que han aceptado formar parte de este proyecto, y por lo tanto realizar la encuesta, aportando su opinión sincera, pertenecen a los siguientes sectores: la administración pública, la hostelería, servicios sociales, periodismo, educación, logística, la abogacía, telemarketing, las TIC, administración, sanidad.

A continuación, se desarrollan las ideas fundamentales, sobre las opiniones que los encuestados han facilitado:

LA ADMINISTRACIÓN PÚBLICA

Las redes sociales generan oportunidades, debido a agilidad e inmediatez en la obtención de la información, y transmisión de datos.

El impacto con respecto a la comunicación interna afecta también, porque crecen de manera exponencial las comunicaciones, sobre todo durante la pandemia en la que vivimos. el impacto de las redes ha sido alto y palpable.

Con respecto a la comunicación externa, se ve como algo necesario, debiendo ser diligente tanto en la protección de datos de los ciudadanos como personas físicas, y como respecto a la vertiente de los datos mercantiles de las personas jurídicas.

En el ámbito de la publicidad, se debe ser prudente ya que se recibe mucha publicidad, sobre todo spam, que puede suponer en ocasiones un colapso de los buzones de correo.

Por último, las relaciones en temas de contratación de servicios, y compras; ha facilitado mucho la gestión de la misma, principalmente como decía en tema de burocracia y de tiempos.

A modo de resumen podemos decir que el punto de riesgo que se ve desde la administración a las redes sociales, es la desprotección de datos personales y secretos mercantiles.

Por ello, las comunicaciones deben estar ordenadas, asignando niveles de prioridad

Un aspecto importante en el que se debe trabajar es la protección de datos y los secretos mercantiles.

SERVICIOS SOCIALES

Las redes sociales generan oportunidades, debido a que la atención al cliente es mucho más rápida y se promociona de una forma directa el catálogo de servicios, identificando los segmentos de la sociedad y por tanto del mercado

Un gran inconveniente, es por el tipo de usuario que reclama los servicios de estos profesionales, el hándicap de no poder llegar a la población que no dispone de conexión a internet.

Con respecto al impacto de las redes sociales, en el ámbito de los servicios sociales, podemos inferir, que en la comunicación interna es una buena manera de que la comunicación sea más fluida en tema de recursos y legislación.

En cuanto a la externa hay mucha mejor proyección al mercado, que hace que este sector se conozca mucho más, sobre todo a través de determinadas redes muy conocidas.

PERIODISMO

Es un escaparate de fácil acceso para cualquier usuario, que genera beneficios para ambas partes; determina la rapidez informativa, y la facilidad para vender productos.

El impacto de las redes sociales, en la comunicación interna, se introducen redes como Slack y el teletrabajo; en cuanto a la comunicación externa, se empieza a valorar la idea de abandonar las webs y centrarse en el uso exclusivo de redes sociales. Tener un buen engagement y cercanía de cara al usuario.

En relación a la publicidad, Es difícil acertar con la publicidad desde el punto de vista creativo, pero ya vemos que con las cookies el usuario está controlado y las redes saben lo que quieren para poner el caramelo. También vemos como se aprovechan influencers o creadores de contenido para vender productos, siendo más efectivo que cualquier spot televisivo.

Con respecto a las compras y ventas, es un escaparate de fácil acceso para cualquier usuario, que tiene beneficios para ambas partes.

Riesgos:

La desinformación, los bulos, debido a que la persona que lo lee no contrasta y da credibilidad a todo lo que lee. Las fake news son un riesgo que debería controlarse; aunque el control es un problema en sí mismo.

TIC

Es una manera muy efectiva de dar a conocer tu empresa al mundo y poder interactuar de forma sencilla con tus clientes.

En la comunicación interna, Creo que la mensajería instantánea se va a convertir en un avance importante dentro de las compañías a la hora de comunicarse con sus empleados y directivos. En comunicación externa, supone que cada vez la tecnología va avanzando más y más y las RRSS se van a convertir en algo imprescindible para cualquier empresa.

En gestión de compras y ventas, En este punto considero que no va a ser tan alto el crecimiento. Se seguirán utilizando seguramente los canales de comunicación habituales.

HOSTELERÍA

En este sector las oportunidades principales son Comunicación, publicidad, retroalimentación…

En relación a la publicidad, Demasiado relevante, establece juicios parciales, rankings ficticios y un exceso de ofertas publicitarias en las que pequeños negocios que no se adapten se desvanecerán.

En la gestión de compras y ventas, Con la desaparición del dinero físico, definitiva.

EDUCACIÓN

Las oportunidades que ofrecen las RRSS Posibilidad de publicitar el negocio y facilidad de contacto tanto con posibles alumnos (clientes) como con profesores. Adaptación a la enseñanza online (vídeos explicativos, exámenes online, etc.).

En relación a la comunicación interna, Representan un método de comunicación cómodo, rápido y gratuito cada vez más utilizado en cualquier ámbito, también dentro de una empresa. y con respecto a la externa, El tipo de clientela de una academia, con un elevado porcentaje de alumnos jóvenes, hace que sean una forma de comunicación cada vez más utilizada, debido al uso natural que ese segmento poblacional hace de redes sociales y mensajería. Además, suponen una herramienta de trabajo.

Y la publicidad que ofrecen. Las redes sociales proporcionan una oportunidad única, y en estos momentos, diría imprescindible, de visibilidad del negocio.

ABOGACÍA.

Entre las oportunidades que ofrecen las RRSS se encuentra, Respecto a las redes sociales en el ámbito de la abogacía cabe destacar que es un medio de publicidad y acceso a clientes que buscan en internet una primera opinión sobre un asunto antes de acudir físicamente a un despacho de un letrado.

Respecto de los medios de mensajería es una herramienta útil entre los abogados, ya que dichas comunicaciones entre ellos está prohibido publicarlas e incluso

utilizarlas en los procedimientos judiciales, al igual que son un medio más o menos seguro de transmisión de documentos entre las partes y entre cliente y abogado.

Con respecto a la comunicación interna, Las RRSS no creo que tengan impacto. Respecto de los medios de mensajería aporta rapidez y *"espacio"* a la hora de almacenar datos de clientes; en referencia a la externa, las RRSS pueden beneficiar al llenar a un gran número de internautas, pero cuidado con tener opiniones contrarias de clientes anteriores. Y los medios de mensajería ayudan a una aportación de documentación entre cliente y abogado, y entre abogados con cierta inmediatez.

GAMING

Principalmente son las redes sociales las que nos permiten mantener una comunidad en contacto. Ya sea a través de plataformas de streaming como Twitch o YouTube para retransmitir nuestro contenido; u otras como discord, twitter o Instagram que complementan los foros que las plataformas de streaming nos ofrecen, pudiendo hacer partícipe a toda la comunidad incluso fuera del horario de las retransmisiones.

Los riesgos provienen principalmente de las redes sociales más que de las plataformas de streaming. La razón es que en las distintas plataformas el foro está regulado y se permite participar a los suscriptores principalmente, mientras que en las redes sociales puedes encontrarte un mayor número de detractores o comentarios tóxicos.

Las RRSS y otros medios de comunicación ya están completamente ligadas a la creación de contenido online, y han sido las grandes responsables del gran impacto y alcance que ahora estamos viendo.

Con respecto a la comunicación interna nos permite estar en contacto entre los distintos miembros del equipo.

En cuanto a la externa, Nos permite darnos a conocer con gran facilidad y que nuestro contenido pueda ser visto en cualquier parte del mundo en tiempo real.

En el campo de la publicidad, como ya he dicho nos permite ampliar a nivel mundial el alcance de nuestras retransmisiones y poder tener suscriptores en todo el mundo.

Y en gestión de compras y ventas, El poder pedir cualquier cosa o vender nuestro merchandising con un solo "clic" sin importar la distancia o el país de origen.

LOGÍSTICA.

La oportunidad de darse a conocer, de hacer comunicados de prensa que lleguen fácilmente al público objetivo, la publicidad, la comunicación interna a los empleados, dar visibilidad a acciones de responsabilidad corporativa, acciones de contratación de personal

Con la información que obtenemos del cuestionario, creo importante y necesario, resaltar las ventajas e inconvenientes del uso de las redes sociales, que estas personas comentan, y que tiene gran influencia en el desempeño de su trabajo.

Mucha de la comunicación interna va a tener lugar en RRSS. En mi empresa durante la pandemia se hacían comunicados internos por Telegram y con ello seguimos

Gran impacto, muchas publicaciones ya tienen lugar en RRSS, sobre todo en RRSS como Linkedin. También la prensa del sector se sigue usando para comunicaciones, aunque es prensa digital.

La publicidad, compaginado RRSS con métodos más tradicionales como Ferias, Mesas Redondas etc…

En la gestión de compras, Creo que menos impacto, aunque también pueden surgir RRSS muy especializadas por ejemplo en servicios de transporte.

TELEMARKETING.

Permite una comunicación rápida y sencilla. Facilita la publicidad, marketing de forma efectiva, debido a que la mayor parte de la documentación en este sector se realiza a través de correo electrónico y por grabación de voz, el papel es algo residual.

En referencia de búsquedas internas relacionadas con productos y servicios, se han implantado muchas aplicaciones específicas para cada uso: coberturas, impagos, etc.

Interacción con empleados más inmediata. Es un paso que se inició hace algún tiempo, las comunicaciones a través de un Messenger propio vía red interna de la empresa.

Facilidad y rapidez en contacto con clientes.

El envío de publicidad se realiza tanto vía correo electrónico como vía WhatsApp. para envío de comunicaciones importantes y personales vía SMS.

Y en publicidad, Mejor y más eficiente forma de dar a conocer productos a las generaciones que son el futuro, vía red social, Facebook, Instagram, etc.

SECTOR PRIMARIO

Sobre todo, información y mayor rapidez.es una de las grandes oportunidades en este sector, tener la información de cada proceso en cada momento, debido a que las aplicaciones se van actualizando constantemente. no es necesario realmente actualizar la información ni la aplicación.

El miedo a perder seguridad e intimidad es uno de los mayores temores, el excesivo número de datos personales y profesionales, que las aplicaciones y programas

requieren para funcionar y para que podamos obtener resultados de ellos. Además de que dejen de ser privados, y a través de consentimientos encubiertos, puedan ser usados por terceros para fines comerciales.

Una de las grandes ventajas, es la rapidez de comunicación con otras personas, gran parte con personas que trabajan en otras explotaciones tanto ganaderas y/o agrícolas, por otra parte, con la red de comerciales que trabajan en este sector, como con clientes finales que vivan en las inmediaciones de la propia comarca.

Todo esto hace que cualquier comunicación sea más cómoda, efectiva; y en consecuencia el negocio sea productivo. En relación a la comunicación interna, es mucho más rápida, debido a que tienen un sistema de comunicación directa.

En la comunicación externa, Una de las grandes ventajas, es la rapidez de comunicación con otras personas, gran parte con personas que trabajan en otras explotaciones tanto ganaderas y/o agrícolas; por otra parte, con la red de comerciales que trabajan en este sector, como con clientes finales que vivan en las inmediaciones de la propia comarca.

Como resumen de todas las aportaciones, a continuación expongo un resumen de ventajas e inconvenientes que presentan las redes sociales.

4.1 Ventajas e inconvenientes.

A continuación, la relación de inconvenientes en primer lugar y ventajas, en segundo lugar.

Inconvenientes:

- ☹ Posibles fraudes en nombre de la empresa.
- ☹ La posibilidad de aparición de bulos o noticias falsas, si no se actúa bien va a trascender a los potenciales clientes (aunque esto último es un riesgo para la empresa, puede ser beneficioso para la sociedad)

☹ Cuidado con las opiniones negativas, que pueden venir por clientes que, a pesar de haber actuado del mejor modo posible, la sentencia ha sido desfavorable, motivo suficiente para ellos de poner una crítica pésima.

☹ En el mundo de la abogacía el riesgo de las redes sociales son las opiniones contrarias vertidas por clientes o/y personas que se hacen pasar por clientes. En mensajería, el principal problema es el respeto a la ley de protección de datos, hay que estar muy seguro de lo que se pueda compartir o no.

☹ Demasiado relevante, establece juicios parciales, rankings ficticios y un exceso de ofertas publicitarias en las que pequeños negocios que no se adapten se desvanecerán.

☹ Excesiva exposición pública, exceso de información no relevante...

☹ La seguridad y el cuidado de la imagen de la compañía

☹ La invasión de la intimidad por el uso de sistemas de mensajería instantánea en el ámbito laboral e incluso la falta de respeto a los horarios de descanso del trabajador.

☹ Consumismo excesivo y *"descontrolado"* (crear en la gente necesidades inexistentes), pérdida de puestos de trabajo y de tiendas *"a pie de calle"*.

☹ El mayor peligro que podemos tener son los virus informáticos o los ciberataques que roben datos personales o que hagan desaparecer documentación importante en nuestras vidas, provocando un pequeño o gran caos.

☹ Pérdida de prestigio por valoraciones negativas con o sin fundamento.

Ventajas:

☺ Facilidad y rapidez en contacto con clientes.

☺ Muy importante también la gestión de la Atención al Cliente y la postventa si se quiere mantener la fidelidad. Hay mucha oferta, mucha competencia y muy buena.

☺ Sin lugar a dudas las RRSS impulsarán el crecimiento de las empresas en cuanto a su publicidad a través de estos medios

☺ Las redes sociales han supuesto un cambio en la comunicación de la Administración con la ciudadanía dando respuesta a los mandatos de transparencia, principio que rige la actuación administrativa.

☺ Se realizan por videoconferencia, lo que supuso una reducción en el uso de tiempo y de recursos.

☺ Y en último lugar, para dejar unas buenas sensaciones, me parece muy interesante y útil, resaltar todos los consejos que estas personas piensan que serían interesantes para tener una mejor relación con las redes sociales, y que afecte de manera positiva a todo aquello que nos rodea.

					
Fraudes		X	Facilidad	X	
Opiniones	X	X	Postventa	X	
Exposición	X	X	Publicidad	X	
Seguridad	X	X	Transparencia	X	
Imagen	X	X	Tiempo	X	X
Consumo	X	X	Control Información	X	X
Desempeño Laboral	X	X	Rapidez	X	X

Como resumen de todas las aportaciones, a continuación, se exponen una lista de consejos que poner en práctica desde las empresas.

4.2 Consejos

- ☞ Buena protección de datos de los ciudadanos tanto a personas físicas, como respecto a la vertiente de los datos mercantiles de las personas jurídicas.
- ☞ Intentar llegar a la población que no dispone de conexión a internet.
- ☞ Las personas deberían formarse más para usar las redes.
- ☞ Desarrollar “la cercanía” de cara al usuario.
- ☞ Invertir de forma importante en seguridad y transmitir a sus posibles clientes tranquilidad y transparencia al respecto
- ☞ La comunicación debe ser clara y precisa. Asimismo, debe ser periódica y proactiva, es decir, conocer las necesidades de información de los usuarios para dar a conocer los actividades y servicios antes de que solicite esa información.
- ☞ Soportarlas sobre una buena red de seguridad.
- ☞ Apostar por un Departamento de Comunicación potente e invertir en acciones diversificadas, pero siempre muy alineadas con el tipo de cliente al que va dirigido su producto o servicio, sin querer estar "en todas partes", en todas las RRSS y plataformas.
- ☞ Un buen asesoramiento previo.
- ☞ Dotarlas de agilidad y respuesta inmediata.
- ☞ Contratar personal cualificado para filtrar y hacer uso de las tecnologías o formación sobre ello para la gestión personal.

- ☞ Que destinen los recursos a redes sociales y marketing. Todavía hay quien lo ve como una prestación menor, pero es imprescindible para llegar a más gente y tener cercanía con el usuario.
- ☞ Mucha precaución a la hora de mantener las redes sociales de la empresa, no solo con segundos factores de autenticación para las cuentas (evitando que estas puedan ser suplantadas), si no también especial cuidado con la imagen que se muestra de ellas mismas en sus perfiles públicos. También es interesante la concienciación de los empleados a la hora del uso de sus propias redes sociales que pudieran afectar de alguna forma a la imagen de la compañía.
- ☞ Exposición a través de las redes sociales de información veraz, precisa y clara de los servicios ofrecidos. Uso de la mensajería responsable, y con ajuste a los horarios laborales.
- ☞ Adecuar el mejor sistema de redes sociales, teniendo en cuenta el perfil del empleado.
- ☞ Que tenga seguridad y sea lo más fácil e intuitivo para los usuarios.
- ☞ Que elija adecuadamente qué redes sociales usar. Cada sector tiene algunas más específicas para su correcto desarrollo y divulgación.
- ☞ *Tener a cargo a una persona especialista que controle todo lo que se publica y con el nivel de seguridad y privacidad requerido.*

Vistas las opiniones de las personas que han realizado el cuestionario, es procedente realizar una pequeña, expuesta en el siguiente apartado.

4.3 Guía de uso de Redes Sociales.

En el presente trabajo se ha comentado en anteriores apartados, y a su vez en los consejos que nos ofrecen las personas encuestadas, las particularidades y requisitos que ellos ven obligatorio o al menos sugerirlos en relación a nuestra forma de trabajar o establecer relación con empresas o trabajos, mediante el uso de internet o las rede sociales.

Después de leer detalladamente las opiniones y consejos de las personas que han participado en el cuestionario, es necesario, como agradecimiento a ellos, y como punto de partida, crear un cuadro al que denominare guía básica de uso para manejar internet.

La guía que se ha confecciona a continuación, lo que pretende es usar internet y las redes sociales en el trabajo. Si bien hay que comentar que la noción básica es la educación y el respeto, por todas aquellas personas que publican información de forma paradójica, temporal o constante.

EMPRESARIO:

Requisitos y procedimientos en comunicación interna

- Invertir de forma importante en seguridad.
- Configurar los dispositivos desde los que se accede de forma remota, a través de una red privada virtual.
- Prever almacenamiento de datos en entorno seguro.
- Establecer aplicaciones y recursos a los que tiene acceso cada usuario.
- Formar a los empleados en el acceso y manejo del entorno de trabajo.
- Acceso a las aplicaciones mediante contraseña.
- Establecer un horario de trabajo, y respetarlo siempre.
- Código ético relación laboral jefe-empleado, respetando tanto horarios, conciliaciones, dignidad, etc.

- Establecer la relación de empleados que tienen autorizado el teletrabajo.
- En el caso de permitir acceder a redes sociales durante las horas de trabajo, definir de manera clara aquellas redes habilitadas, la duración, los dispositivos, y horarios.
- Indicar de forma clara y concisa, la información interna que se pueda publicar.
- Contratar a los mejores profesionales en cada campo.

Funcionalidades en comunicación externa

- Tener al cargo a una persona especialista que controle todo lo que se publica y con el nivel de seguridad y privacidad requerido.
- Realizar una planificación de acciones a realizar.
- Disponer de herramientas analíticas.
- Elegir los canales adecuados para la empresa.
- Tener objetivos realistas en cuanto a seguidores.
- Tener los datos de los clientes en un almacenamiento protegido.
- Que tenga seguridad y sea lo más fácil e intuitivo para los usuarios.
- Destinar los recursos a redes sociales y marketing
- Transmitir a sus posibles clientes tranquilidad y transparencia al respecto
- Desarrollar “la cercanía” de cara al usuario.

TRABAJADOR:

Como empleado.

- Aprovechar los cursos de formación facilitados, a tal fin.
- Cumplimiento de la normativa propuesta para el teletrabajo.
- Acceso a las aplicaciones mediante contraseña habilitado al efecto.

- No usar los mecanismos a disposición para objetivos diferentes a los establecidos.
- Código ético relación laboral jefe-empleado, respetando tanto horarios, conciliaciones, dignidad, etc.
- La identificación de aquella información que se puede publicar, enviar, y el medio al que envía o en el que se publica. Y, por consiguiente, identificar la información privada, y la de publicación prohibida.
- Ser siempre profesional en lo que se envía.
- Ser responsable con el tratamiento de la información a la que se tiene acceso, y la que deriva del desempeño laboral.
- Hacer hincapié en el respeto mutuo, propio y ajeno.
- Respetar siempre el horario de trabajo.

Como usuario de redes sociales.

- Comparte la información cierta, si no está seguro no la comparta.
- Corrobore la información, que pretenda compartir.
- Procure buscar la información en fuentes fiables y en más de un medio.

CONCLUSIONES

En un mundo globalizado como en el que vivimos, la vida transcurre a una velocidad inimaginable en la que han sucedido todo tipo de cambios y transformaciones que no nos son indiferentes, por el contrario, todos estamos afectados por ellos, de una manera u otra. En este cambio entran en juego, varios participantes; por una parte, instituciones, pymes y ciudadanos; y por la otra parte, internet y las redes sociales. Es por esto que el presente trabajo trata de reflejar en un golpe de vista, la influencia y el impacto que tienen internet y las redes sociales en nuestras vidas.

La expresión “en nuestras vidas”, nos involucra no solamente como ciudadanos en un momento y lugar determinados, sino como personas que coexisten en una sociedad con características sociales determinadas, trabajo, familias, vida social, etc. Para poder hacer ese pequeño análisis, mi foco de atención se fijará en cómo afecta internet y las redes sociales en nuestra vida profesional, y de manera más concreta en las pymes que integran los diferentes sectores de actividad económica.

A la hora de abordar este proyecto, en un primer momento me centré en recopilar datos, sobre la gran transformación que hemos experimentado durante la pandemia, planteándome de forma inocente, que era el comienzo de esta gran odisea, pero nada más lejos de la realidad. Todo este proceso había comenzado mucho antes, y a las pruebas me remito, en el capítulo primero realizo una pequeña investigación sobre los orígenes de internet, se produce a partir de los 90, cuando se hizo pública la red de internet global, con el World Wide Web (lo que, comúnmente conocemos como «www.»), en este momento nacería Internet**,** y como consecuencia de ello años más tarde las redes sociales actuales.

El estudio realizado es solo una pequeña muestra de lo que podría ser una gran investigación de las redes sociales, porque los avances e innovaciones se producen de forma frenética, sin haber logrado dominar el uso de una aplicación, aparecen varias diferentes.

Para entender este trabajo es importante y preciso valorar el tremendo impacto en la vida económica, que tienen las TIC. Su evolución y desarrollo, incluye las numerosas particularidades y beneficios que pueden tener para los diferentes sectores de la actividad económica. Para comprobarlo, una parte de la pequeña investigación que he realizado en webs oficiales, ha facilitado una relación de estudios y la información sobre todas las novedades en internet y redes sociales, que siguen las empresas para mantenerse al día, que es el Ciberespacio. La otra parte corresponde al cuestionario que forma parte de este trabajo.

Pese a las buenas intenciones de las que se parten, se debe ser consciente y reconocer que realizar este trabajo ha sido duro y sorprendente, y esto se debe a la

amplísima información por la red, y no es fácil clarificar cuál podría considerarse válida y por el contrario cuál no. Por lo que este trabajo también trata de este tema, extraer una información que no está a simple vista por la tremenda complejidad que supone internet. La guía que se confecciona, parte de ese mismo caos, en el que nos encontramos todos los profesionales que queremos encontrar información consistente y seria en la red.

En todo trabajo también es preciso valorar los puntos débiles, para ser conscientes de que siempre hay posibilidad de mejora, y en el trabajo la principal debilidad puede ser el reconocimiento, de que he efectuado una encuesta menos profesional de lo habitual, es decir no se elabora una encuesta siguiendo los pasos pertinentes, secuenciados; ni se realiza a un grupo de personas elevado sacando muestras, etc. En este caso se preferido que las personas encuestadas, dieran una opinión sincera y expresando su malestar y gratitud hacia las redes sociales; lo que cambiarían si tuviesen posibilidad de hacerlo, también lo que mejorarían, y los consejos para todas aquellas personas que participan en las redes.

Bien es cierto, observando el desarrollo del estudio realizado, ahora que trabajo en la administración pública que hay alguna referencia y algún consejo en la guía de buen uso de la Administración Publica, con respecto al uso de herramientas para la conexión ciudadano-administración. Por lo que este trabajo peca de un profundo análisis de un elemento que posee la administración, y sería de digno de una intensa evaluación; que en este trabajo no voy a poder llevar a cabo, el BIG DATA. Con ese término se denomina la estructura organizada y desarrollada por la administración, para la recopilación de datos, muchos de los cuales pone al servicio tanto de otras administraciones como de los ciudadanos, para un manejo más provechoso y eficaz, de su relación con la administración, y por ende de su día a día.

El desconocimiento de la administración pública, y su potencial gracias al Big Data, la dota de cantidad de información disponible para ayudar dentro de la misma entidad y por supuesto al ciudadano, creando una web y sus perfiles en redes sociales, para ponérselo más sencillo al ciudadano. Pero como decía, si no sabes buscar, es complicado encontrar.

Como aporte adicional se podía haber incluido un estudio más exhaustivo de las aplicaciones Facebook e Instagram, las actualmente conocidas como aplicaciones de empresa para publicitarse de forma más rápida en las redes sociales, pero son estudios que ya se han realizado y que, por extensión, sobrepasaría los estándares de este trabajo. Por ello, como apunte en el capítulo 2 hago una sucinta referencia a una aplicación analíticas que aportan el feedback que es necesario para mejorar en cualquier sector profesional. La aplicación es Facebook Insights Realiza un análisis directo de la actividad en Facebook, es efectividad y de fácil comprensión.

En resumidas cuentas, con Facebook Insights podríamos desde entender mejor a nuestros usuarios, Aprovechar los contenidos que más afinidad tengan, analiza y monitorea a la competencia, realizar tus propios análisis, analiza y comprende tu demografía y para finalizar, Aprovecha tus mejores publicaciones para saber la mejor hora para publicar.

Como es sabido existe por la red gran cantidad de información, que publica todo tipo de personas. La información publicada es accesible a toda persona que se conecte a la red. La amplísima información por la red, y no es fácil clarificar cuál podría considerarse válida y por el contrario cuál no.

Una nueva situación que está provocando las redes sociales, es el hecho de que un porcentaje de población de ambos sexos esté descontenta con las redes sociales, y comiencen a tener pensamientos de desvincularse de las redes sociales, los motivos y justificaciones de esta nueva manera de pensar están basados en una casuística determinada, en la que no vamos a entrar.

Como vemos en el capítulo cuatro, las redes sociales tienen su lado positivo y también negativo, la tabla realizada en este capítulo muestra de forma resumida las ventajas e inconvenientes que el uso por parte de las personas, puede ocasionar.

Una mala opinión puede destrozar un negocio, y una buena, levantarlo. Todo está vinculado a una buena o mala praxis.

Es por esto, que en este capítulo realizo una guía de buenas prácticas, para que seamos conscientes de lo que es recomendable y ético, de cómo actuar en el día a día desde nuestra posición en las redes. Muy pocas opiniones iguales pueden ser muy beneficiosas o muy dañinas.

Se ha convertido en el nuevo modelo, es decir, desde que comenzó la pandemia sufrimos muchos estragos en todos los sectores profesionales, y como consecuencia las empresas que por características y capacidad pusieron en práctica esta nueva forma de trabajo casi desconocida en nuestro país, fueron poco a poco saliendo del abismo en el que todas entraron.

La cantidad de profesionales involucrados en adaptar todas las herramientas, para que sean intuitivas, y de fácil manejo. Podemos ver una pequeña muestra en la siguiente tabla, que nos muestra la evolución de los profesionales contratados para hacerse cargo de esta sección de la empresa.

Año	2012	2016	2020
España	6	12	12
Europa	7	8	7
	85%	150%	171%

Tabla 1: profesionales contratados para gestionar redes sociales. Fuente: elaboración propia. ONTSI

Por último, mencionar de nuevo la parte importante de este trabajo, aunque no tan mencionada como las ventajas e inconvenientes. Es la nueva concepción del mundo laboral, la nueva forma de desarrollar nuestra profesión, el teletrabajo.

El teletrabajo se había implantado en nuestro país de forma anecdótica, y desde que comenzó la pandemia se ha incrementado de manera visible, por lo que sede las instituciones han creído conveniente crear una regulación estatal (se incluye anexo, en el que se incluya a todas las personas que desarrollen su actividad profesional en este país. De esta manera se trata de evitar todo tipo de abusos.

REFERENCIAS BIBLIOGRÁFICAS

Cocktail. *"Acerca de Tiktok: Nuestra Misión".* https://www.tiktok.com/about?lang=es)

"Cómo crear un cuestionario". Cefire. Tema 3. Módulos interactivos. http://cefire.edu.gva.es/file.php/1/moodle/T3_MInteractivos/42_crear_un_cuestionario.html

Derek L. Hansen, Ben Shneiderman, Marc A. Smith, Itai Himelboim (2020), *"Analyzing Social Media Networks with NodeXL (Second Edition). Insights from a Connected World"*- Social media: New technologies of collaboration, (Pages 11-29). https://www.sciencedirect.com/science/article/pii/B9780128177563000029,

De La Hera, C. (2021). *"Historia de las Redes Sociales: cómo nacieron y cuál fue su evolución"*., Marketing4ecommerce. https://marketing4ecommerce.net/historia-de-las-redes-sociales-evolucion/)

Estudio de redes sociales 2021. IAB España. https://iabspain.es/estudio/estudio-de-redes-sociales-2021/

Indicadores de uso de inteligencia artificial en las empresas españolas. Red.es. Ontsi. https://www.ontsi.red.es/es/dossier-de-indicadores-pdf/indicadores-uso-inteligencia-artificial-empresas-espanolas

Instagram Marketing (2021). https://cocktailmarketing.com.mx/instagram-marketing/)

Instituto Nacional de Ciberseguridad. ¿Qué es incibe? https://www.incibe.es/que-es-incibe

Juste, M. (2021). *"La pandemia dispara el uso de las redes sociales, un 27% más que hace un año".* Expansión. Economía digital. https://www.expansion.com/economia-digital/innovacion/2021/02/10/6022c89de5fdea59448b459b.html

Ministerio de Industria, Comercio y Turismo Cifras PYME. Datos enero 2021. Ministerio de Industria, Comercio y Turismo. http://www.ipyme.org/Publicaciones/CifrasPYME-enero2021.pdf

Miñana, C. *"Facebook Insight, la mejor herramienta para medir".* https://www.publicidadenlanube.es/facebook-insights-tutorial-espanol/

MIT Institute for Data *"Ciberseguridad en el teletrabajo Una guía de aproximación para el empresario"*. MIT Institute for Data, Systems, and Society. https://idss.mit.edu/research/research-domains/social-networks/

Observatorio Nacional de Tecnología y la Sociedad (2021). Indicadores de uso de Inteligencia Artificial en las empresas españolas. Madrid: Ministerio de Asuntos Económicos y Transformación Digital, Secretaria General Técnica. https://www.ontsi.red.es/es/dossier-de-indicadores-pdf/indicadores-uso-inteligenciaartificialempresas-espanolas.

Ortiz, D. (2019). *"El fundador de Telegram, sobre WhatsApp: «Ni un día ha sido seguro»"*. Hipertextual. https://hipertextual.com/2019/05/pavel-durov-telegram-whatsapp-seguro)

Ponce, I. (2012) *"Monográfico: Redes Sociales"*. Observatorio Tecnológico. Ministerio de Educación, Cultura y Deporte. http://recursostic.educacion.es/observatorio/web/ca/internet/web-20/1043-redes-sociales

Telegram: Una nueva era de mensajería. https://telegram.org/

Gráficos y Tablas:

Encuesta sobre uso de redes sociales

Sector Profesional *

Administración Pública

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Inmediatez en la transmisión y agilidad en la obtención de información.

Cuáles cree que son los principales riesgos *

La protección de datos y secretos mercantiles.

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

Muy altas. La Administración ha de tecnificarse para ofrecer unos servicios modernos y ágiles pero ha de simplificar procedimientos y trámites.

Comunicación interna *

Por supuesto que en las comunicaciones internas las TIC's están presentes y cada vez con mayor uso.

Comunicación externa *

Necesaria, sin perjuicio de la debida diligencia y cuidado en la protección de datos de los ciudadanos, tanto en su vertiente de persona física como los datos mercantiles en la vertiente de persona jurídica.

Publicidad *

Uso excesivo de publicidad no requerida o spam, que puede suponer en determinadas ocasiones colapso de los buzones de e-mail.

Gestión de compras y ventas *

Muy útil y facilita la gestión del tiempo.

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Las comunicaciones deben estar ordenadas, asignando niveles de prioridad, cuestión que las comunicaciones electrónicas permiten con total sencillez, pero que puede permitir gestionar de manera racional la información que se transmita, pero exigiendo un riguroso compromiso de no usarse para cuestiones ajenas a su fin. Evitar los contenidos banales y debe estar basado en la sencillez y claridad de ideas, cuestión en modo alguno opuesta a formalismos de educación y respeto.

Encuesta sobre uso de redes sociales

Sector Profesional *

Servicios Sociales

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Atención al cliente más rápida y directa de la promoción de los servicios. Identificación de los segmentos de mercado.

Cuáles cree que son los principales riesgos *

No llegar a la población que no maneje internet. Estar expuesto a más críticas.

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

Tendrá que ver ensucomunicacion interna y externa. En su política corporativa

Comunicación interna *

Nueva manera de trasladar a su plantilla una comunicación más fluidas. Con sus riesgos

Comunicación externa *

Mercado más amplio. Mundo globalizado. Proyección de mercado

Publicidad *

Instagramer

Gestión de compras y ventas *

Expansión del mercado

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Contratar a expertos

Encuesta sobre uso de redes sociales

Sector Profesional *

Periodismo

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Es un escaparate de fácil acceso para cualquier usuario, que tiene beneficios por ambas partes. Por un lado la rapidez informativa y, para las empresas, mayor facilidad de vender sus productos.

Cuáles cree que son los principales riesgos *

La desinformación, los bulos virales... la gente no contrasta y da credibilidad a todo lo que ve. Las fake news son un riesgo que debería controlarse; aunque el control de la información en sí mismo es un problema. La gente quizás debería formarse más para usar redes.

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

Las RRSS han llegado para quedarse como herramienta de venta y comunicativa. Evolucionarán y las empresas deben adecuarse a su público para no estancarse

Comunicación interna *

Ya se han instaurado por medio de redes como Slack y teniendo en cuenta el teletrabajo derivado por la pandemia, estas evolucionarán en acceso más rápido o video conferencias

Comunicación externa *

Muchas empresas van a terminar prescindiendo de webs y van a limitar su comunicación solamente en redes. Con un buen engagement con los usuarios, cercanía y demás bastaría con tener una plataforma para adquirir los productos si se diera el caso.

Publicidad *

Es difícil acertar con la publicidad desde el punto de vista creativo pero ya vemos que con las cookies el usuario está controlado y las redes saben lo que quieren para poner el caramelo. También vemos como se aprovechan influencers o creadores de contenido para vender productos, siendo más efectivo que cualquier spot televisivo.

Gestión de compras y ventas *

Un poco el resumen de lo mencionado en anteriores puntos.

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Que destinen los recursos a redes sociales y marketing. Todavía hay quien lo ve como una prestación menor pero es imprescindible para llegar a más gente y tener cercanía con el usuario.

Encuesta sobre uso de redes sociales

Sector Profesional *

Periodismo

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Es un escaparate de fácil acceso para cualquier usuario, que tiene beneficios por ambas partes. Por un lado la rapidez informativa y, para las empresas, mayor facilidad de vender sus productos.

Cuáles cree que son los principales riesgos *

La desinformación, los bulos virales... la gente no contrasta y da credibilidad a todo lo que ve. Las fake news son un riesgo que debería controlarse; aunque el control de la información en sí mismo es un problema. La gente quizás debería formarse más para usar redes.

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

Las RRSS han llegado para quedarse como herramienta de venta y comunicativa. Evolucionarán y las empresas deben adecuarse a su público para no estancarse

Comunicación interna *

Ya se han instaurado por medio de redes como Slack y teniendo en cuenta el teletrabajo derivado por la pandemia, estas evolucionarán en acceso más rápido o video conferencias

Comunicación externa *

Muchas empresas van a terminar prescindiendo de webs y van a limitar su comunicación solamente en redes. Con un buen engagement con los usuarios, cercanía y demás bastaría con tener una plataforma para adquirir los productos si se diera el caso.

Publicidad *

Es difícil acertar con la publicidad desde el punto de vista creativo pero ya vemos que con las cookies el usuario está controlado y las redes saben lo que quieren para poner el caramelo. También vemos como se aprovechan influencers o creadores de contenido para vender productos, siendo más efectivo que cualquier spot televisivo.

Gestión de compras y ventas *

Un poco el resumen de lo mencionado en anteriores puntos.

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Que destinen los recursos a redes sociales y marketing. Todavía hay quien lo ve como una prestación menor pero es imprescindible para llegar a más gente y tener cercanía con el usuario.

Encuesta sobre uso de redes sociales

Sector Profesional *

Administración Pública

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Permite una comunicación interna inmediata y que la publicidad de las actuaciones llegue a mas personas

Cuáles cree que son los principales riesgos *

La invasión de la intimidad por el uso de sistemas de mensajería instantánea en el ámbito laboral e incluso la falta de respeto a los horarios de descanso del trabajador.

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

En concreto en la Administración ha supuesto un impulso en el conocimiento de la actividad administrativa y en la puesta en marcha de la Administración electrónica.

Comunicación interna *

Las comunicaciones internas se llevan a cabo a través de correo electrónico y las reuniones, antes presenciales, ahora se realizan por videoconferencia, lo que supuesto una reducción en el uso de tiempo y de recursos.

Comunicación externa *

Las redes sociales han supuesto un cambio en la comunicación de la Administración con la ciudadanía dando respuesta a los mandatos de transparencia, principio que rige la actuación administrativa. Todas las actuaciones deben ser expuestas y conocidas por los ciudadanos y para ello, las redes sociales ha supuesto la vía principal de comunicación.

Publicidad *

La actividad de la Administración esta sujeta al principio de publicidad activa, lo que exige un portal web que recoja las iniciativas y actividades que lleva a cabo, el Junta de Castilla y León es el portar GOBIERNO ABIERTO. Resultaría muy complicado dar publicidad de las actividades sin el uso de estos medios electrónicos.

Gestión de compras y ventas *

no se

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

La comunicación debe ser clara y precisa. Asimismo, debe ser periódica y proactiva, es decir, conocer las necesidades de información de los usuarios para dar a conocer los actividades y servicios antes de que solicite esa información.

Encuesta sobre uso de redes sociales

Sector Profesional *

Sanitario

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Publicidad

Cuáles cree que son los principales riesgos *

Los hackers

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

Mucha

Comunicación interna *

Muy importante

Comunicación externa *

Importante

Publicidad *

Muy importante

Gestión de compras y ventas *

Muy importante

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Soportarlas sobre una buena red de seguridad
Un buen asesoramiento previo.
Dotarlas de agilidad y respuesta inmediata.

Encuesta sobre uso de redes sociales

Sector Profesional *

Ofimatica

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Conocimiento productos servicios y empresas

Cuáles cree que son los principales riesgos *

Las falsas opiniones

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

Positivo por la presencia en nuestro día a día

Comunicación interna *

Positivo

Comunicación externa *

Positivo

Publicidad *

Positivo

Gestión de compras y ventas *

Positiva

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Claridad y brevedad

Encuesta sobre uso de redes sociales

Sector Profesional *

TIC

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Es una manera muy efectiva de dar a conocer tu empresa al mundo y poder interactuar de forma sencilla con tus clientes

Cuáles cree que son los principales riesgos *

La seguridad y el cuidado de la imagen de la compañía

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

A continuación en cada una de ellas

Comunicación interna *

Creo que la mensajería instantánea se va a convertir es un avance importante dentro de las compañías a la hora de comunicarse con sus empleados y directivos

Comunicación externa *

Supongo que cada vez la tecnología va avanzando más y más y las RRSS se van q convertir en algo imprescindible para cualquier empresa

Publicidad *

Sin lugar a dudas las RRSS impulsarán el crecimiento de las empresas en cuanto a su publicidad a través de estos medios

Gestión de compras y ventas *

En este punto considero que no va a ser tan alto el crecimiento. Se seguirán utilizando seguramente los canales de comunicación habituales

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Mucha precaución a la hora de mantener las redes sociales de la empresa, no solo con segundos factores de autenticación para las cuentas (evitando que estas puedan ser suplantadas), si no también especial cuidado con la imagen que se muestra de ellas mismas en sus perfiles públicos. También es interesante la concienciación de los empleados a la hora del uso de sus propias redes sociales que pudieran afectar de alguna forma a la imagen de la compañía

Encuesta sobre uso de redes sociales

Sector Profesional *

TIC

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Es una manera muy efectiva de dar a conocer tu empresa al mundo y poder interactuar de forma sencilla con tus clientes

Cuáles cree que son los principales riesgos *

La seguridad y el cuidado de la imagen de la compañía

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

A continuación en cada una de ellas

Comunicación interna *

Creo que la mensajería instantánea se va a convertir es un avance importante dentro de las compañías a la hora de comunicarse con sus empleados y directivos

Comunicación externa *

Supongo que cada vez la tecnología va avanzando más y más y las RRSS se van q convertir en algo imprescindible para cualquier empresa

Publicidad *

Sin lugar a dudas las RRSS impulsarán el crecimiento de las empresas en cuanto a su publicidad a través de estos medios

Gestión de compras y ventas *

En este punto considero que no va a ser tan alto el crecimiento. Se seguirán utilizando seguramente los canales de comunicación habituales

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Mucha precaución a la hora de mantener las redes sociales de la empresa, no solo con segundos factores de autenticación para las cuentas (evitando que estas puedan ser suplantadas), si no también especial cuidado con la imagen que se muestra de ellas mismas en sus perfiles públicos. También es interesante la concienciación de los empleados a la hora del uso de sus propias redes sociales que pudieran afectar de alguna forma a la imagen de la compañía

Encuesta sobre uso de redes sociales

Sector Profesional *

Hostelería

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Comunicación, publicidad, retroalimentación...

Cuáles cree que son los principales riesgos *

Excesiva exposición pública, exceso de información no relevante...

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

esta respuesta sobra

Comunicación interna *

Imprescindible

Comunicación externa *

Relevante

Publicidad *

Demasiado relevante, establece juicios parciales, rankings ficticios y un exceso de ofertas publicitarias en las que pequeños negocios que no se adapten se desvanecerán.

Gestión de compras y ventas *

Con la desaparición del dinero físico, definitiva

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

¡Corred insensatos! (Contratar personal cualificado para filtrar y hacer uso de las tecnologías o formación sobre ello para la gestión personal)

Encuesta sobre uso de redes sociales

Sector Profesional *

Administración Pública

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Las RRSS han permitido democratizar la publicidad que necesitan las empresas y personas para dar a conocer sus productos/servicios globalemente sin las importantes inversiones que requieren los medios "clásicos" (prensa, TV, etc). La mensajería ha hecho más fácil y rápido el acceso a todo tipo de productos.

Cuáles cree que son los principales riesgos *

Consumismo excesivo y "descontrolado" (crear en la gente necesidades inexistentes), pérdida de puestos de trabajo y de tiendas "a pie de calle"

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

Importante y definitivo. Los cambios han llegado para quedarse

Comunicación interna *

Menor que en la externa

Comunicación externa *

Cambio importantísimo. Hay que estar al día de todo lo que es publicidad on line estar en las plataformas que más convengan en cada caso y trabajarlas a fondo, creando contenido interesante y atractivo para los potenciales clientes estando en comunicación constante con él y midiendo siempre los retornos de ese esfuerzo comunicativo

Publicidad *

idem. Si no te publicitas, si no te ven, no existes

Gestión de compras y ventas *

Fundamental para conseguir la agilidad que los clientes y usuarios demandan. Domina el "lo veo, lo quiero...y lo quiero ya!". Muy importante también la gestión de la Atención al Cliente y la postventa si se quiere mantener la fidelidad. Hay mucha oferta, mucha competencia y muy buena.

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Apostar por un Departamento de Comunicación potente e invertir en acciones diversificadas pero siempre muy alineadas con el tipo de cliente al que va dirigido su producto o servicio, sin querer estar"en todas partes", en todas las RRSS y plataformas.

Encuesta sobre uso de redes sociales

Sector Profesional *

Administración

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

En mi trabajo lo que nos da servicio es la mensajería. Constituye un sistema esencial a la hora de interactuar con el resto de compañeros, y sobre todo en este ultimo año, debido a la situación sanitaria, se ha convertido en una herramienta imprescindible a la hora de intercambiar información y de desarrollo laboral. Los documentos en papel van siendo relegados a un segundo plano frente a la documentación virtual que se mueve con mucha mayor facilidad

Cuáles cree que son los principales riesgos *

El mayor peligro que podemos tener son los virus informáticos o los ciberataques que roben datos personales o que hagan desaparecer documentación importante en nuestras vidas, provocando un pequeño o gran caos

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

Creo que llevamos unos años en los que las redes sociales y la informática en general, se han ido imponiendo en nuestras vidas de forma espectacular.
 En el terreno laboral va a ser y es algo inevitable, pero en lo personal, nos estamos empezando a volver mas recelosos de nuestra intimidad y cada vez buscamos nuevos programas y sistemas que nos garanticen la privacidad de los datos que compartimos, para asegurarnos que acceden a ellos solo quienes nosotros queremos que lo haga. Nos estamos concienciando del valor que tienen los datos personales y lo que damos a conocer sobre nuestras vidas, gustos, aficiones etc...sin darnos cuenta

Comunicación interna *

No se a que se refiere la pregunta

Comunicación externa *

No se a que se refiere la pregunta

Publicidad *

La cantidad de publicidad con la que nos bombardean cada vez que accedemos a internet, relacionada "casualmente", con nuestras ultimas consultas, es una de las cosas que nos hacen ser conscientes de lo "controlados/manipulados" que podemos llegar a estar

Gestión de compras y ventas *

En muchas ocasiones nos resulta muy muy cómodo gestionar nuestras compras, ocio y demás a través de las redes sociales. Es un sistema que se esta imponiendo con fuerza, pero al que veo inconvenientes en cuanto que vamos dejando nuestros datos bancarios por un montón de sitios, no siempre suficientemente seguros, lo que nos puede suponer mas de un disgusto. Del mismo modo, este "nuevo comercio", esta haciendo mucho daño al tradicional, y a nosotros mismos que compramos en la mayoría de los casos mucho mas q antes, tentados por las "supuestas" ofertas, que muchas veces no son tales, y sobre todo por la comodidad de poder hacerlo en cualquier momento y lugar

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Invertir de forma importante en seguridad y transmitir a sus posibles clientes tranquilidad y transparencia al respecto

Encuesta sobre uso de redes sociales

Sector Profesional *

Hosteleria

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Buenas

Cuáles cree que son los principales riesgos *

La mala publicidad y el mal uso

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

Pueden ayudar o pueden undir el negocio

Comunicación interna *

Si

Comunicación externa *

Si

Publicidad *

Es necesario

Gestión de compras y ventas *

También es necesario

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Sacrificio e ilusion

Encuesta sobre uso de redes sociales

Sector Profesional *

Enseñanza en una academia; actualmente modalidad online

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Posibilidad de publicitar el negocio y facilidad de contacto tanto con posibles alumnos (clientes) como con profesores. Adaptación a la enseñanza online (vídeos explicativos, exámenes online, etc.)

Cuáles cree que son los principales riesgos *

Pérdida de prestigio por valoraciones negativas con o sin fundamento.

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

Alto. Sobre todo por la implementación de la enseñanza online en este último año.

Comunicación interna *

Representan un método de comunicación cómodo, rápido y gratuito cada vez más utilizado en cualquier ámbito, también dentro de una empresa.

Comunicación externa *

El tipo de clientela de una academia, con un elevado porcentaje de alumnos jóvenes , hace que sean una forma de comunicación cada vez más utilizada, debido al uso natural que ese segmento poblacional hace de redes sociales y mensajería. Además suponen una herramienta de trabajo.

Publicidad *

Las redes sociales proporcionan una oportunidad única, y en estos momentos, diría imprescindible, de visibilidad del negocio.

Gestión de compras y ventas *

Apartado no relacionado con mi área de trabajo.

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Exposición a través de las redes sociales de información veraz, precisa y clara de los servicios ofrecidos. Uso de la mensajería responsable, y con ajuste a los horarios laborales.

Encuesta sobre uso de redes sociales

Sector Profesional *

ABOGACÍA

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Respecto a las redes sociales en el ámbito de la abogacía cabe destacar que es un medio de publicidad y acceso a clientes que buscan en internet una primera opinión sobre un asunto antes de acudir físicamente a un despacho de un letrado.
Respecto de los medios de mensajería es una herramienta útil entre los abogados, ya que dichas comunicaciones entre ellos está prohibido publicarlas e incluso utilizarlas en los procedimientos judiciales, al igual que son un medio más o menos seguro de transmisión de documentos entre las partes y entre cliente y abogado.

Cuáles cree que son los principales riesgos *

En el mundo de la abogacía el riesgo de las redes sociales son las opiniones contrarias vertidas por clientes o/y personas que se hacen pasar por clientes. En mensajería, el principal problema es el respeto a la ley de protección de datos, hay que estar muy seguro de lo que se pueda compartir o no.

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

Escasa

Comunicación interna *

Las RRSS no creo que tengan impacto. Respecto de los medios de mensajería aporta rapidez y "espacio" a la hora de almacenar datos de clientes

Comunicación externa *

las RRSS pueden beneficiar al llenar a un gran número de internautas, pero cuidado con tener opiniones contrarias de clientes anteriores. Y los medios de mensajería ayudan a una aportación de documentación entre cliente y abogado, y entre abogados con cierta inmediatez.

Publicidad *

Puede ser positiva para conocer tu despacho, pero como he mencionado antes, cuidado con las opiniones negativas, que pueden venir por clientes que a pesar de haber actuado del mejor modo posible, la sentencia ha sido desfavorable, motivo suficiente para ellos de poner una crítica pésima.

Gestión de compras y ventas *

No influye casi nada en la abogacía, lo único que se puede conseguir los suministros de oficina por medios telemáticos.

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Ponerse en manos de un especialista en el tema.

Encuesta sobre uso de redes sociales

Sector Profesional *

Logística

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

La oportunidad de darse a conocer, de hacer comunicados de prensa que lleguen fácilmente al público objetivo, la publicidad, la comunicación interna a los empleados, dar visibilidad a acciones de responsabilidad corporativa, acciones de contratación de personal

Cuáles cree que son los principales riesgos *

La posibilidad de aparición de bulos o noticias falsas, si no se actúa bien va a trascender a los potenciales clientes (aunque esto último es un riesgo para la empresa, puede ser beneficioso para la sociedad)

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

Respondo por punto

Comunicación interna *

Mucha de la comunicación interna va a tener lugar en RRSS. En mi empresa durante la pandemia se hacían comunicados internos por Telegram y con ello seguimos

Comunicación externa *

Gran impacto, muchas publicaciones ya tienen lugar en RRSS, sobre todo en RRSS como Linkedin. También la prensa del sector se sigue usando para comunicaciones, aunque es prensa digital

Publicidad *

Igual que en el punto anterior, compaginado RRSS con métodos más tradicionales como Ferias, Mesas Redondas etc...

Gestión de compras y ventas *

Creo que menos impacto, aunque también pueden surgir RRSS muy especializadas por ejemplo en servicios de transporte

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Tener al cargo a una persona especialista que controle todo lo que se publica y con el nivel de seguridad y privacidad requerido

Encuesta sobre uso de redes sociales

Sector Profesional *

Telemarketing

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Permite una comunicación rápida y sencilla .Facilita la publicidad ,marketing de forma efectiva.

Cuáles cree que son los principales riesgos *

Posibles fraudes en nombre de la empresa.

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

Impacto positivo

Comunicación interna *

Interacción con empleados mas inmediata.

Comunicación externa *

Facilidad y rapidez en contacto con clientes.

Publicidad *

Mejor y mas eficiente forma de dar a conocer productos a las generaciones que son el futuro.

Gestión de compras y ventas *

Inmediatez en todo lo relacionado con este departamento.

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Adecuar el mejor sistema de redes sociales ,teniendo en cuanta el perfil del empleado.

Encuesta sobre uso de redes sociales

Sector Profesional *

AGRICOLA

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

SOBRE TODO INFORMACION Y MAYOR RAPIDEZ

Cuáles cree que son los principales riesgos *

EL MIEDO A PERDER SEGURIDAD E INTIMIDAD (QUE LOS DATOS TUYOS DEJEN DE SER PRIVADOS)

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

SOBRE TODO LA RAPIDEZ EN COMUNICARTE CON OTRAS EMPRESAS RELACIONADAS CON TU SECTOR, U MAZYOR COMODIDAD

Comunicación interna *

MAYOR RAPIDEZ DENTRO DE LA EMPRESA

Comunicación externa *

TAMBIEN MAYOR RAPIDEZ COMO HE COMENTADO ANTES

Publicidad *

LLEGA CON MUCHA RAPIDEZ

Gestión de compras y ventas *

CADA VEZ SE UTILIZA MAS

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

qUE TENGA SEGURIDAD Y QUE SEA LOS MAS FACIL E INTUITIVO PARA LOS USUARIOS

Encuesta sobre uso de redes sociales

Sector Profesional *

Gaming

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Principalmente son las redes sociales las que nos permiten mantener una comunidad en contacto. Ya sea a traves de plataformas de streaming como twitch o youtube para retransmitir nuestro contenido; u otras como discord, twitter o instagram que complementan los foros que las plataformas de streaming nos ofrecen, pudiendo hacer participe a toda la comunidad incluso fuera del horario de las retransmusiones.

Cuáles cree que son los principales riesgos *

Los riesgos provienen principalmente de las redes sociales mas que de las plataformas de streaming. La razon es que en las distintas plataformas el foro esta regulado y se permite oarticipar a los subscriptores principalmente, mientras q en las redes sociales puedes encontrarte un mayor numero de detractores o comentarios toxicos.

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

Las RRSS y otros medios de comunicacion ya estan completamente ligadas a la creacion de contenido online, y han sido las grandes responsables del gran impacto y alcance que ahora estamis viendo.

Comunicación interna *

Nos permite estar en contacto entre los distintos miembros del equipo.

Comunicación externa *

Nos permite darnos a conocer con gran facilidad y que nuestro contenido pueda ser visto en cualquier parte del mundo en tiempo real.

Publicidad *

Como ya he dicho nos permite ampliar a nivel mundial el alcance de nuestras retransmisiones y poder tener subscriptores en todo el mundo.

Gestión de compras y ventas *

El poder pedir cualquier cosa o vender nuestro merchandising con un solo "clic" sin importar la distancia o el pais de origen.

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Que elija adecuadamente que redes sociales usar. Cada sector tiene algunas mas especificas para su correcto desarrollo y divulgacion.

Encuesta sobre uso de redes sociales

Sector Profesional *

Informática

Cuáles son en su opinión las principales oportunidades que proveen las redes sociales y la mensajería al mundo de la empresa *

Networking y dar conocimiento de empresas al mayor número de gente posible

Cuáles cree que son los principales riesgos *

El contenido no es fácilmente controlable. La anonimidad no ayuda.

Qué impacto cree que van a tener las RRSS y los sistemas de comunicación en las siguientes dimensiones de la vida de la empresa *

Altísimo

Comunicación interna *

No muy alta. Las comunicaciones internas suelen seguir otras vías de comunicación.

Comunicación externa *

Muy alta. Llegan a mucha gente.

Publicidad *

Altísima. Mi opinión es que es el motivo principal.

Gestión de compras y ventas *

No muy alta.

Qué consejos daría a una empresa para gestionar de manera adecuada sus comunicaciones *

Tener un buen CM que tenga libertad y apoyo. No es nada fácil.

Ciberseguridad en el teletrabajo

Una guía de aproximación para el empresario

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa

ÍNDICE

ÍNDICE

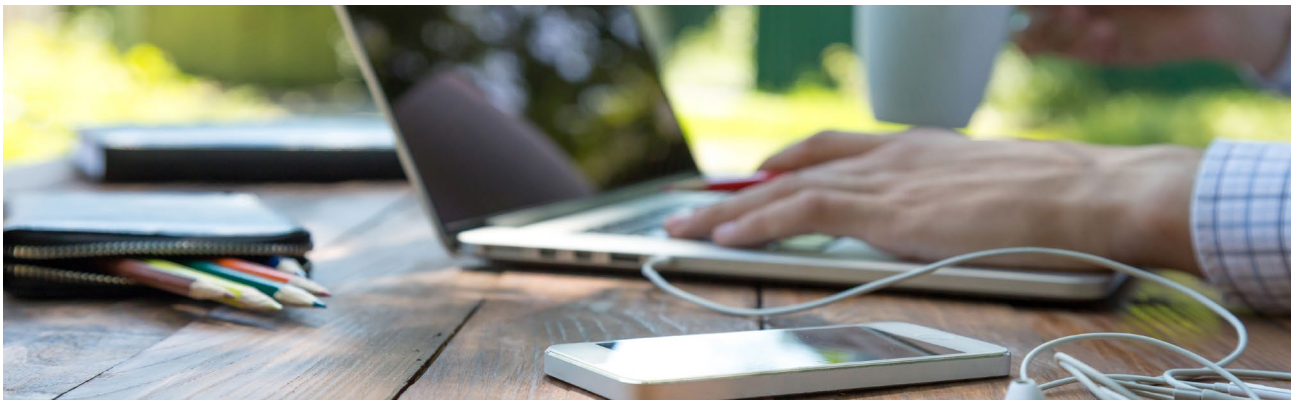
1 INTRODUCCIÓN

Se puede definir el teletrabajo como la actividad laboral que se desarrolla desde otros lugares que no sean las propias instalaciones de la organización.

Los teletrabajadores pueden utilizar varios terminales también conocidos como *endpoints*, como ordenadores de sobremesa, portátiles, teléfonos inteligentes o tabletas, para leer y enviar correo electrónico, acceder a sitios web, crear y editar documentos, así como otras muchas tareas propias de su labor diaria. Estos dispositivos pueden ser controlados por la organización, por terceros (contratistas/prestadores de servicios, interlocutores comerciales o proveedores de la organización) o por los propios usuarios cuando utilizan sus dispositivos para trabajar, lo que se conoce como BYOD[1]. La seguridad del teletrabajo también se ve afectada por el uso de estos dispositivos y de otros medios de almacenamiento extraíbles (memorias usb, discos duros, etc.), así como por el uso de aplicaciones en la nube y mecanismos de acceso remoto a la red y servidores de la empresa.

La mayoría de los teletrabajadores utilizan el acceso remoto (a través de VPN, escritorio remoto, etc.), lo que permite que los usuarios de una organización puedan acceder a los recursos informáticos de la empresa desde ubicaciones externas distintas de las instalaciones de la empresa.

A lo largo de este documento explicaremos las distintas medidas necesarias para garantizar conexiones remotas seguras, proteger los dispositivos de teletrabajo, el uso seguro de la nube y las herramientas colaborativas y la seguridad en movilidad.



1 El modo de trabajo en el que se permite la utilización de dispositivos móviles personales para acceder y utilizar los recursos corporativos es lo que se conoce como BYOD (por sus iniciales en inglés, Bring Your Own Device, tráete tu propio dispositivo). Para más información consulta: Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario

2 POLÍTICA DE TELETRABAJO

Si queremos disponer de un entorno de teletrabajo seguro, el primer paso será establecer una política organizativa en la que se definan las normas a cumplir en los distintos escenarios o respecto al uso de los distintos sistemas y métodos de acceso. Esta política deberá contemplar distintos aspectos, como los siguientes, siempre teniendo en cuenta que cada organización tendrá sus necesidades particulares. Estos son algunos elementos que ha de definir esta política:

- **Relación de usuarios que disponen de la opción de trabajar en remoto.** Será necesario llevar un control de las personas que por su perfil dentro de la empresa o las características de su trabajo tienen la opción de teletrabajar.

- **Procedimientos para la solicitud y autorización del teletrabajo.**

- **Aplicaciones y recursos a los que tiene acceso cada usuario.** Cada usuario tendrá acceso solo a las aplicaciones y recursos que requiera para realizar su trabajo, dependiendo del rol que desempeñe en la empresa. Se detallarán las aplicaciones colaborativas y de teleconferencia permitidas así como sus condiciones de uso evitando utilizar programas no controlados por la empresa, práctica conocida como Shadow IT[2] .

- **Mecanismos de acceso seguro mediante contraseña.** Para las credenciales de acceso se utilizarán siempre contraseñas robustas y el doble factor de autenticación siempre que sea posible, y forzando su cambio periódico. Este mecanismo puede estar ligado a la gestión de cuentas de usuario y control de accesos a través de servicios de directorio[3] LDAP[4] .

- **Configuración que deberán tener los dispositivos desde los que se establezcan las conexiones remotas:** sistema operativo, antivirus, control de actualizaciones, etc., tanto si son corporativos como si son aportados por el trabajador (BYOD). En el caso del BYOD, podemos controlar su configuración a través del *fingerprinting* de dispositivos, es decir, registrando una «huella di-

2 El término Shadow IT engloba dispositivos, *software y servicios de TI utilizados dentro de las organizaciones y los cuales se encuentran fuera de su propiedad o control*

3 Un servicio de directorio (SD) es una aplicación o un conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de ordenadores y sobre los recursos de red que permite a los administradores gestionar el acceso de usuarios a los recursos sobre dicha red. https://es.wikipedia.org/wiki/Servicio_de_directorio

4 El protocolo ligero de acceso a directorios (en inglés: Lightweight Directory Access Protocol, también conocido por sus siglas de LDAP) hace referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. https://es.wikipedia.org/wiki/Protocolo_ligero_de_acceso_a_directorios

2

"Si queremos disponer de un **entorno de teletrabajo seguro**, el primer paso será establecer una **política organizativa** en la que se definan las normas a cumplir en los distintos escenarios o respecto al uso de los distintos sistemas y métodos de acceso."

gital» del dispositivo autorizado generada con datos de uso: navegador y ***plugins*** instalados, operador de telefonía, ubicación, horarios, etc.).

» **Procedimiento y tecnología para cifrar los soportes de información** para proteger los datos de la empresa de posibles accesos malintencionados y garantizar así su confidencialidad e integridad.

» **Definición de la política de almacenamiento en los equipos de trabajo [REF - 1] así como de almacenamiento en la red corporativa [REF - 2].**

» **Procedimiento y planificación de las copias de seguridad periódicas de todos los soportes** y comprobar regularmente que pueden restaurarse.

» **Uso de conexiones seguras a través de una red privada virtual** o VPN, del inglés *Virtual Private Network*, en lugar de las aplicaciones de escritorio remoto. De este modo, la información que intercambiamos entre nuestros equipos viaja cifrada a través de Internet. Se ha de evitar el uso de aplicaciones de escritorio remoto si no es a través de una VPN. Estas herramientas pueden crear puertas traseras *(backdoors*[5]*)* **[REF - 3]** a través de las cuales podría comprometerse el servicio o las credenciales de acceso de usuario y por lo tanto permitir el acceso a los equipos corporativos. Además, al usar este tipo de aplicaciones podemos estar aceptando ciertos términos y condiciones de uso que podrían otorgar algún tipo de «privilegio» a las mismas sobre nuestros equipos e información.

» **Virtualización**[6] **de entornos de trabajo** para eliminar los riesgos asociados al uso de un dispositivo propio.

» En el caso de utilizar dispositivos móviles para teletrabajar, la política debe incluir **la utilización de aplicaciones de administración remota [REF - 4].** Definir los criterios para evitar el uso de redes wifi públicas y utilizar las conexiones 4G/5G en su lugar.

» **Formar a los empleados [REF - 5]** antes de empezar a teletrabajar.

5 Puerta trasera: Se denomina *backdoor* o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema.

6 La virtualización es la creación a través de software de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento o cualquier otro recurso de red. https://es.wikipedia.org/wiki/Virtualización

3 OBJETIVOS DE SEGURIDAD EN EL ACCESO REMOTO

Tanto si trabajamos en las instalaciones de la empresa como si teletrabajamos, debemos proteger el principal activo de la organización, **la información.** La seguridad de la información se articula sobre cinco dimensiones, que son los pilares sobre los que aplicar las medidas de protección:

- **Disponibilidad:** asegurar que los usuarios puedan acceder a los recursos cuando lo necesiten.
- **Autenticidad:** garantizar los procesos de autenticación y control de acceso para que solo las personas autorizadas puedan acceder a la información.
- **Integridad:** proteger la exactitud y estado completo de la información detectando cualquier cambio intencional o no intencional en las comunicaciones.
- **Confidencialidad:** asegurar que los datos almacenados por el usuario o en tránsito en las comunicaciones no puedan ser leídos por partes no autorizadas.
- **Trazabilidad:** establecer los procedimientos y mecanismos para proporcionar los datos necesarios que permitan llevar a cabo un análisis de seguridad en caso de sufrir un incidente.

Además de estas consideraciones, debemos tener en cuenta las principales leyes que afectan a la empresa desde el punto de vista de la seguridad de la información y cumplir con lo estipulado en las mismas **[REF - 6]**:

- La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE).
- La Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) y el Reglamento General de Protección de Datos (RGPD).
- La Ley de Propiedad Intelectual (LPI).

3

"Tanto si trabajamos en las instalaciones de la empresa como si teletrabajamos, debemos **proteger el principal activo de la organización, la información.**"

Para lograr estos objetivos de seguridad, todos los componentes de las soluciones de teletrabajo y acceso remoto, incluyendo los dispositivos cliente[7], los servidores de acceso remoto y los servidores internos a los que se accede a través del acceso remoto, deben estar configurados correctamente para minimizar las posibles **amenazas** que se detallan a continuación:

- **Falta de controles de seguridad física:** en ciertas ocasiones los dispositivos destinados al teletrabajo se utilizan en lugares fuera de la organización como por ejemplo en hoteles, cafeterías, en salas de conferencias, etc. Esta condición aumenta el riesgo de que los dispositivos se pierdan o sean robados, lo que lo convierte a su vez en una posible pérdida de datos corporativos si no están convenientemente protegidos. Es muy importante tener en cuenta este tipo de situaciones a la hora de aplicar las medidas de seguridad necesarias para este tipo de dispositivos y proteger la información de accesos no deseados. **[REF - 7]**

- **Errores de configuración:** para asegurar una configuración óptima en nuestros equipos es aconsejable que únicamente el personal técnico indicado pueda instalar, actualizar y eliminar *software*.

- **Redes no seguras:** las organizaciones no tienen control sobre las redes que usan sus empleados para teletrabajar. Es una práctica habitual utilizar redes abiertas e inseguras (aeropuertos, cafeterías, etc.) que un ciberdelincuente podría aprovechar para acceder a la información que contiene el dispositivo utilizado para el trabajo en remoto.

- **Dispositivos infectados en redes corporativas:** la inclusión del BYOD en el ámbito empresarial ha sumado factores de riesgo, como el uso de dispositivos que están infectados con algún tipo de *malware* a consecuencia del uso personal. El problema surge cuando una vez infecta-

7 La arquitectura **cliente-servidor** es un modelo de diseño de software en el que las tareas se reparten entre los proveedores de recursos o servicios, llamados **servidores**, y los demandantes, llamados **clientes**. Un cliente realiza peticiones a otro programa, el **servidor**, quien le da respuesta. https://es.wikipedia.org/wiki/Cliente-servidor

3

dos se conectan a la red de la empresa, pudiendo propagar el *malware* a otros dispositivos.

- **Acceso remoto a los recursos internos:** permitir el acceso externo a los recursos corporativos implica su exposición a nuevas amenazas, aumentando la posibilidad de que estos se vean comprometidos. Por este motivo, es necesario otorgar acceso a estos recursos solo a los empleados que lo necesiten para el desempeño de su trabajo.

- **Falta de formación:** es habitual que la falta de formación o de conocimiento de las políticas de seguridad de la empresa por parte de los empleados pongan en riesgo la seguridad de la información.

4 MÉTODOS DE ACCESO REMOTO

Existen varias opciones para proporcionar acceso remoto a los empleados de una organización, siendo las más utilizadas VPN, VDI, acceso a través de escritorio remoto, portales de aplicaciones y acceso directo a aplicaciones.

Al planificar qué solución de acceso remoto es la más adecuada para nuestra empresa, se deben considerar cuidadosamente las implicaciones de seguridad de cada método y si cumple con los requisitos de seguridad necesarios para llevar a cabo las tareas corporativas que van a realizarse en remoto.

A continuación detallamos dichos métodos y sus principales medidas de seguridad.

4.1. VPN

Una red privada virtual, también conocida por sus siglas VPN *(Virtual Private Network)*, es una tecnología de red que permite una extensión segura de una red local (LAN[8]) sobre una red pública o no controlada como Internet.

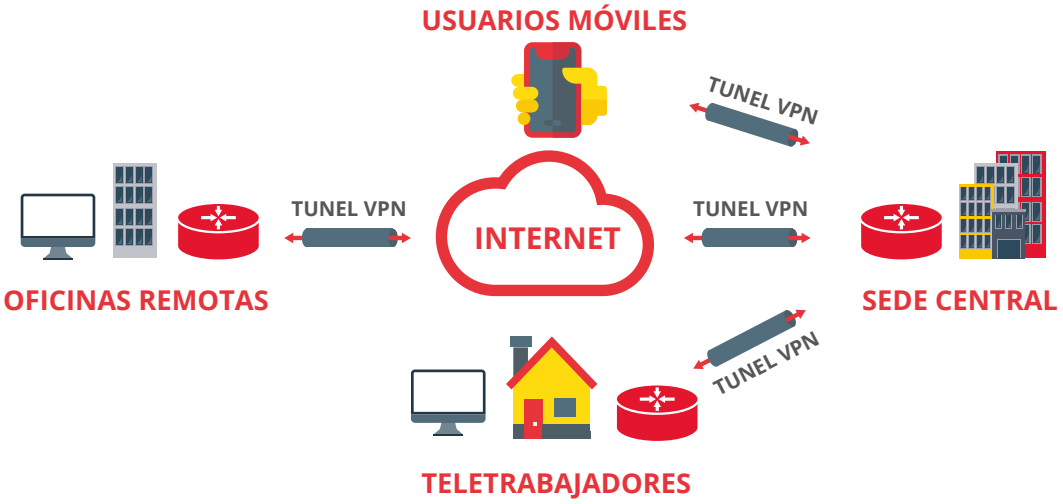


Ilustración 1 Estructura de una VPN para una empresa

8 Una red de área local o LAN (por las siglas en inglés de *Local Area Network*) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.

4

Las conexiones establecidas utilizando VPN protegen la información que se intercambia, ya que establecen un «túnel» o canal cifrado de comunicación entre nuestro dispositivo y nuestro lugar de trabajo por donde «viajan» nuestros datos confidenciales de manera segura. El *software* VPN cifra la información enviada por los dispositivos, lo que significa que no se puede interceptar el tráfico que se está transmitiendo a través de Internet.

Este sistema funciona aplicando una clave de cifrado a los datos para transformarlos de forma que resulten indescifrables. La información sólo puede ser descifrada por un sistema que también tenga la clave utilizada para cifrar los datos (clave secreta previamente compartida), lo que significa que las redes VPN son bastante difíciles de descifrar. La mayoría de los sistemas VPN en la actualidad ofrecen cifrado AES-256 **[REF - 8]**.

"Al establecer una VPN, la **integridad** de los datos y la **confidencialidad** se protegen mediante la autenticidad del cliente, es decir, sólo se permite el acceso a los usuarios autorizados y el cifrado, dificultando que un tercero pueda robar información confidencial."

Al establecer una VPN, la **integridad** de los datos y la **confidencialidad** se protegen mediante la autenticidad del cliente, es decir, sólo se permite el acceso a los usuarios autorizados y el cifrado, dificultando que un tercero pueda robar información confidencial. Además de proteger la confidencialidad y la integridad las VPN proporcionan:

- **Autenticación mutua:** proceso por el cual dos partes de una comunicación se identifican y autentican una a la otra simultáneamente, garantizando la legitimidad de los participantes en la comunicación.
- **Protección frente a reenvíos:** asegurando que los datos solo se entregan una vez, evitando la posibilidad de que sean interceptados por un ciberdelincuente o que este inserte paquetes maliciosos en la comunicación.
- **La protección frente al análisis de tráfico:** impidiendo que se pueda extraer información a través del análisis de la comunicación (los datos que se transmiten entre los dos extremos, la cantidad de datos transmitidos, etc.)

Como bien sabemos, nada garantiza la seguridad al cien por cien. Si bien el uso de estas redes reduce el riesgo significativamente, existen factores que afectan a su seguridad como una implementación poco robusta, vulnerabilidades en el *software*, que la clave de acceso se vea comprometida, etc. Por estos motivos, siempre se debe estar al día de las posibles amenazas **[REF - 9]** y salvaguardar la **información**.

4

4.2. Arquitecturas VPN

En términos simples, una VPN crea un "túnel de comunicación" que une cliente y servidor para mantener una comunicación segura y privada entre ellos. Posibilita la ampliación de la red de la empresa haciendo que los recursos informáticos de una ubicación estén disponibles para los empleados de otras ubicaciones.

Se debe valorar las necesidades de seguridad y recursos de tu empresa para decidir si la implementación puede llevarse a cabo por el personal técnico, o por el contrario deber contratarse como un servicio externo **[REF - 11]**. En los siguientes puntos explicaremos los escenarios de VPN más comunes y sus principales características técnicas.

"En términos simples, una VPN crea un **"túnel de comunicación"** que une cliente y servidor para mantener una comunicación segura y privada entre ellos. "

4.2.1. VPN de sitio a sitio

También conocida como VPN *Site-To-Tite* (por su denominación en inglés). Esta implementación se utiliza principalmente para comunicar un sitio con uno o más sitios remotos (por ejemplo, la sede principal de la empresa y una sede secundaria) a través de una red pública como Internet, estableciendo una conexión segura.

En este escenario, los dispositivos cliente (terminales) no necesitan ningún *software* VPN, ni precisan ningún tipo de configuración adaptada para el uso de la misma. Requiere de dos dispositivos servidores VPN, uno en cada sitio que se quiera conectar.

Existen dos tipos de implementaciones VPN de sitio a sitio:

- **Basada en intranet:** si una empresa tiene una o más ubicaciones remotas a las que desea unirse en una sola red privada puede crear una VPN de intranet para conectar cada LAN separada a una sola WAN[9].

- **Basada en extranet:** cuando una compañía tiene una relación cercana con otra compañía (como un socio, proveedor o cliente), puede construir una extranet VPN que conecte las LAN de esas compañías. Esta extranet VPN permite a las empresas trabajar juntas en un entorno de red seguro y compartido, a la vez que impide el acceso a sus intranets independientes.

9 Una red de área amplia, o WAN (*Wide Area Network* en inglés), es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física.

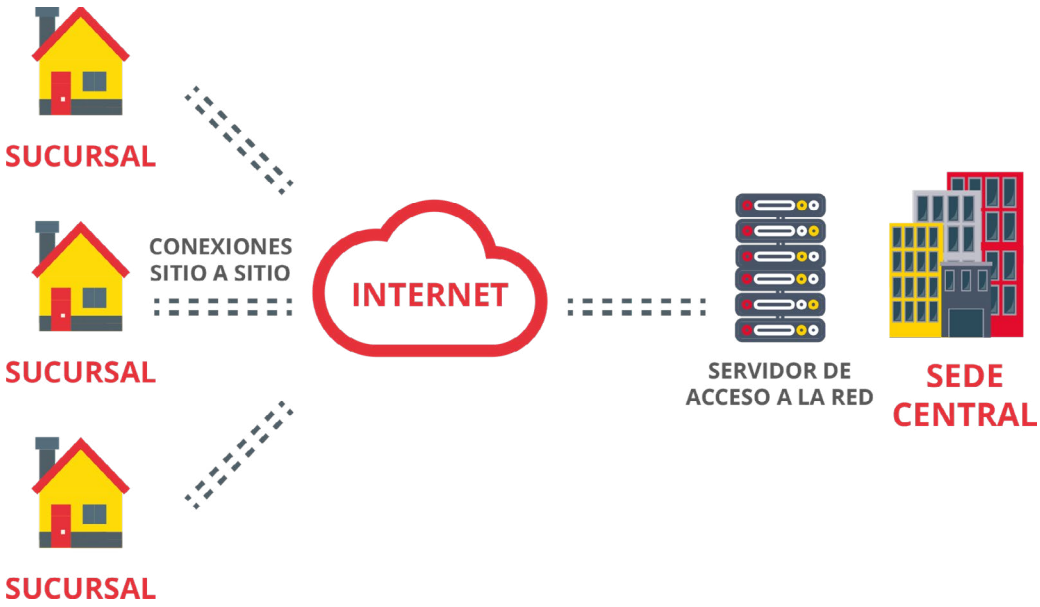


Ilustración 2: VPN de sitio a sitio basada en Intranet

4.2.2. VPN de acceso remoto

Se utiliza principalmente para salvaguardar las comunicaciones entre el dispositivo del teletrabajador y la red interna de la empresa. Se puede utilizar este tipo de VPN para hacer que una red de oficina esté disponible de forma remota para los usuarios autorizados, como por ejemplo los empleados que trabajan desde casa o en el transcurso de un viaje, y por tanto necesitan acceder de forma remota a las aplicaciones y a la información corporativas utilizando Internet como vínculo de acceso.

Esta configuración requiere de dos dispositivos:

- Un dispositivo *hardware* instalado en la red de la organización, denominado concentrador de VPN o VPN *Gateway*, que conecta la red de la organización con los clientes VPN de forma segura.

- Un dispositivo *software* o cliente VPN en el lado del usuario que conecta de forma segura a los dispositivos cliente, como por ejemplo ordenadores o *smartphones* de empleados que trabajan en remoto, con las redes de la organización.

Estas dos arquitecturas pueden funcionar bajo distintos protocolos VPN. Para ampliar información consulta este enlace **[REF - 12]**.

Ilustración 3: VPN de acceso remoto

4.3 Cómo saber si una VPN es confiable

Una vez analizadas las necesidades de nuestra organización y antes de tomar la decisión final sobre la VPN que vamos a implantar, debemos leer atentamente las condiciones de contratación y la política de privacidad. Estas son algunas recomendaciones:

- Antes de confiar en una VPN **debemos informarnos**, consultar quién la ofrece, las **condiciones del servicio**, su funcionamiento, su rendimiento, etc.

- Revisaremos también la **compatibilidad** con el sistema operativo utilizado en la organización y con los navegadores además de verificar su **escalabilidad** es decir, cuántas conexiones permite.

- Si se trata de una aplicación para el móvil, **habrá que revisar los permisos** que solicita para su instalación, su nivel de aceptación y buscar información sobre su desarrollador. No se deben instalar aplicaciones que soliciten accesos excesivos a tus datos o a datos que nada tengan que ver con el servicio.

- Seleccionaremos una VPN que **cifre todo el tráfico y que cifre extremo a extremo**. Hay VPN que cifran sólo hasta su servidor o que sólo cifran determinado tipo de tráfico **[REF - 11]**.

- Lee con detenimiento la **política de privacidad** sobre todo si comparten información con terceros. Escogeremos preferentemente para usos profesionales VPN no gratuitas y sin publicidad. Las aplicaciones gratuitas suelen requerir permisos para compartir los datos de la organización con terceros con el objeto de enviar anuncios.

- Comprobaremos que tenemos personal formado para su **auditoría y mantenimiento** o que nuestro proveedor TI **[REF - 10]** ofrece estos servicios.

4

4.4 Infraestructura de escritorio virtual o VDI

Una infraestructura de escritorio virtual, o VDI por sus siglas en ingles *Virtual Desktop Infrastructure*, es una tecnología que consiste en virtualizar **[REF - 13]** los entornos de trabajo de los empleados y alojarlos en una ubicación controlada por la empresa. Este tipo de solución encaja tanto para situaciones de teletrabajo en las que gran parte de la plantilla está fuera de la oficina, como también cuando habitualmente hay trabajadores con una elevada movilidad, como comerciales, flotas de reparto, soporte in situ, etc.

Para el empleado es muy similar a trabajar desde su puesto en la oficina ya que puede disponer del mismo sistema operativo y aplicaciones con las que ya trabajaba pero desde cualquier dispositivo: ordenadores portátiles, *smartphones* o *tablets*, **accediendo** a su entorno de trabajo personal generalmente a través de un navegador web.

"Una infraestructura de escritorio virtual, o VDI por sus siglas en ingles Virtual Desktop Infrastructure, es una tecnología que consiste en **virtualizar los entornos de trabajo** de los empleados y alojarlos en una ubicación controlada por la empresa."

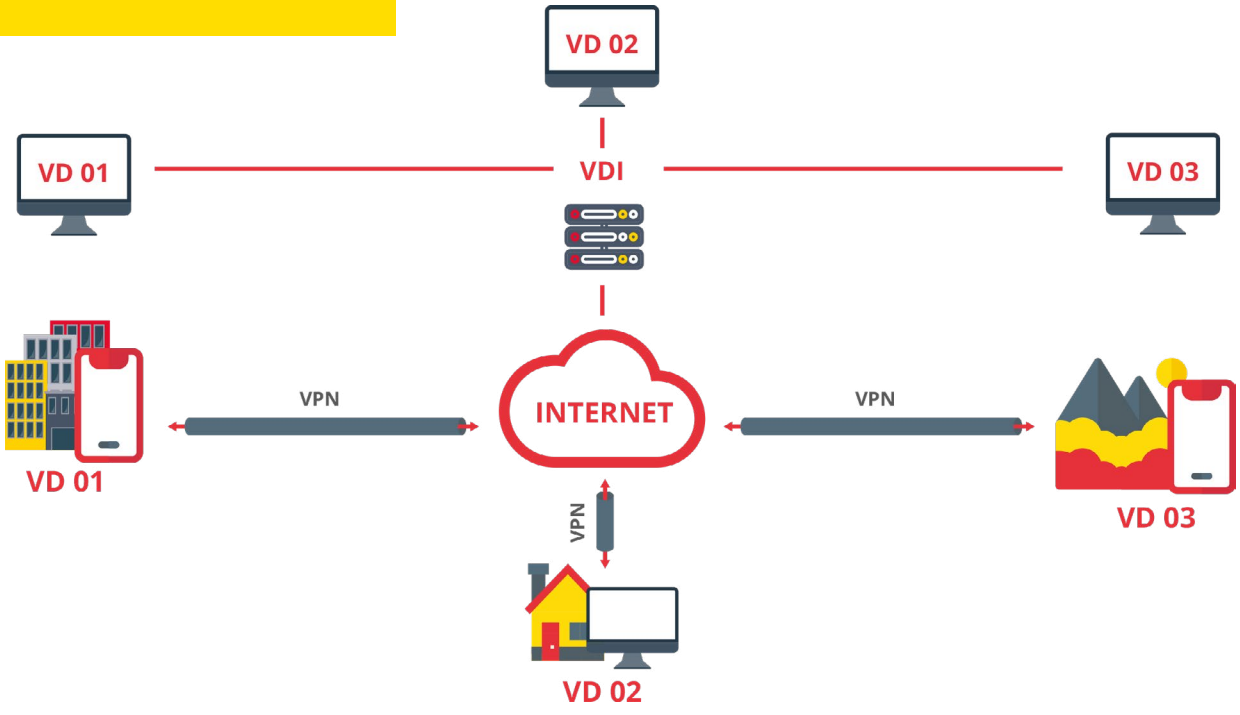


Ilustración 4: Infraestructura de escritorio virtual o VDI

4

"**Los entornos de trabajo de los empleados son gestionados por la empresa** mediante la solución VDI elegida , pudiendo estar alojada en un servidor propio o en los servidores de una empresa contratada según las necesidades de la organización."

4.4.1. VDI propio o como servicio «DaaS»

Los entornos de trabajo de los empleados son gestionados por la empresa mediante la solución VDI elegida, pudiendo estar alojada en un servidor propio o en los servidores de una empresa contratada según las necesidades de la organización.

- **Instalar VDI en un servidor propio:** su principal ventaja es el control sobre la administración del sistema evitando depender de terceros **[REF - 14]** a los que trasladar nuestros requisitos de seguridad. No obstante, hay que contar con personal técnico que realice la implementación, así como considerar el tiempo de despliegue y el gasto económico que conlleva la adquisición de *hardware*.

- **VDI como servicio o DaaS *(Desktop as a Service)*:** consiste en contratar a una empresa externa todo lo relacionado con la puesta en marcha y mantenimiento del sistema VDI. Los escritorios virtuales de los empleados pueden seguir siendo gestionados internamente y así aplicar las mismas medidas y políticas de seguridad que si el VDI estuviera ubicado en un servidor propio. El principal inconveniente de este modelo es que la privacidad de la información gestionada puede verse comprometida. Para evitarlo, además de leer detenidamente la política de privacidad y seguridad del servicio contratado, tendremos que detallar nuestros requisitos de seguridad y privacidad y firmar un acuerdo de nivel de servicio.

4.5. Ventajas de utilizar un sistema VDI

Ya sea propio de la empresa o contratado como servicio, presenta varias ventajas frente a otros sistemas de teletrabajo.

4.5.1. Movilidad

Los sistemas VDI son adecuados para entornos con elevada movilidad, como es el caso de comerciales, técnicos, altos cargos, etc. Estos trabajadores dispondrán de un entorno de trabajo igual al que tendrían en un dispositivo corporativo desde cualquier ubicación con acceso a Internet.

Además, disponer de un sistema VDI en la empresa puede permitir a los empleados realizar teletrabajo desde sus casas sin comprometer la seguridad de la empresa y la información que gestiona.

4

"**Ventajas de utilizar un sistema VDI** Ya sea propio de la empresa o contratado como servicio, presenta varias ventajas frente a otros sistemas de teletrabajo."

4.5.2. Entorno seguro

Los sistemas VDI son entornos de trabajo seguros, ya que los escritorios de los empleados son controlados por la empresa. Cualquier política de seguridad que se aplique a los dispositivos físicos de la organización **[REF - 15]** puede trasladarse a los escritorios virtuales de los empleados.

La información que se gestiona en los escritorios virtuales está bajo las mismas medidas de seguridad que si se trabajara en dispositivos físicos. En todo momento la información está alojada en servidores controlados por la empresa y no es almacenada en el dispositivo utilizado para teletrabajar.

4.5.3. Ahorro de costes

Los sistemas VDI requieren de una menor inversión económica en el *hardware* utilizado comparado con otros sistemas de teletrabajo. Esto se debe a que todas las herramientas necesarias son ejecutadas en el servidor, por lo que la carga de trabajo de los dispositivos es pequeña. Además permitiría a la empresa implementar una política de BYOD, *Bring Your Own Device* **[REF - 16]**, con el consecuente ahorro en terminales.

Por otro lado, el despliegue de escritorios virtuales también es un proceso relativamente sencillo que requiere poco tiempo, lo que se traduce en un menor gasto de tiempo para el personal técnico de la organización.

4.5.4 . Escalabilidad

Los sistemas VDI se caracterizan por ofrecer una elevada escalabilidad, adaptándose a las circunstancias cambiantes de la empresa con más flexibilidad que otras opciones. Si se requiere aumentar el número de puestos de trabajo, el administrador puede crear nuevos escritorios virtuales, y cuando este volumen de trabajo descienda, podrá eliminarlos también de forma sencilla. Además, también puede asignar más recursos a un empleado si puntualmente los necesita.

4

"Ya que las tecnologías móviles están cada vez más presentes en el entorno empresarial, **la infraestructura móvil virtual (VMI)** es una muy buena opción a considerar a la hora de mejorar la seguridad en nuestra organización."

4.5.5. Consideraciones de seguridad en el uso de VDI

Medidas de seguridad relativas al control de acceso y a las comunicaciones:

- Cuando se habilita en la empresa un sistema VDI, el control de acceso por parte de los usuarios debe ser lo más robusto posible, para evitar accesos no autorizados al sistema. Para ello el acceso debería contar con doble factor de autenticación **[REF - 17],** como puede ser el uso de dispositivos o aplicaciones que generan una contraseña de un solo uso u OTP (del inglés *One Time Password*). De esta manera se reduce el riesgo de que un tercero sin autorización acceda al sistema.

- La utilización de redes privadas virtuales o VPN es la solución ideal para proteger las comunicaciones entre el dispositivo del empleado y el escritorio virtual evitando posibles fugas de información.

4.6. VMI

Ya que las tecnologías móviles están cada vez más presentes en el entorno empresarial, la infraestructura móvil virtual (VMI) es una muy buena opción a considerar a la hora de mejorar la seguridad en nuestra organización.

Aunque el acceso al servidor de terminales y las tecnologías VDI están destinadas principalmente a los equipos de teletrabajo, existe una tecnología emergente que proporciona capacidades similares para los dispositivos móviles: la infraestructura móvil virtual (VMI). Así como una solución VDI proporciona un escritorio virtual seguro a un ordenador de teletrabajo, también VMI facilita un entorno de dispositivo móvil virtual seguro a un dispositivo móvil de teletrabajo. Una infraestructura móvil virtual permite acceder a aplicaciones móviles remotas desde un dispositivo móvil. Como las aplicaciones se ejecutan en servidores corporativos, no es posible perder sus datos o que los roben, incluso si se pierde el dispositivo o es sustraído.

Resulta muy útil para separar entornos de trabajo y personales en un mismo dispositivo. Es además muy práctico si un empleado deja su puesto de trabajo ya que la empresa sólo tiene que bloquearle el acceso al sistema remoto y toda la información corporativa deja de ser accesible para ese usuario.

4

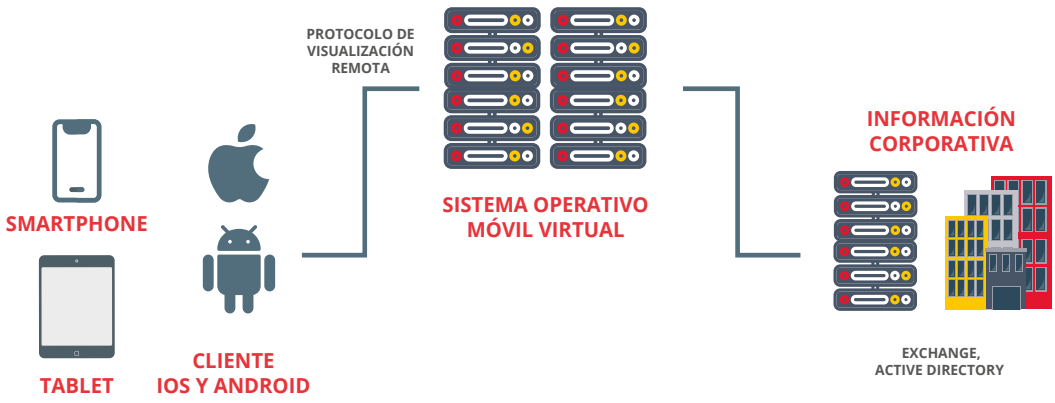


Ilustración 5: infraestructura VMI

4.7. Aplicaciones de escritorio remoto

Las aplicaciones de acceso de escritorio remoto **[REF - 19]** proporcionan al teletrabajador la posibilidad de controlar remotamente un equipo, siendo habitual conectarse al equipo del que se es usuario en la oficina de la organización, desde un dispositivo cliente de teletrabajo.

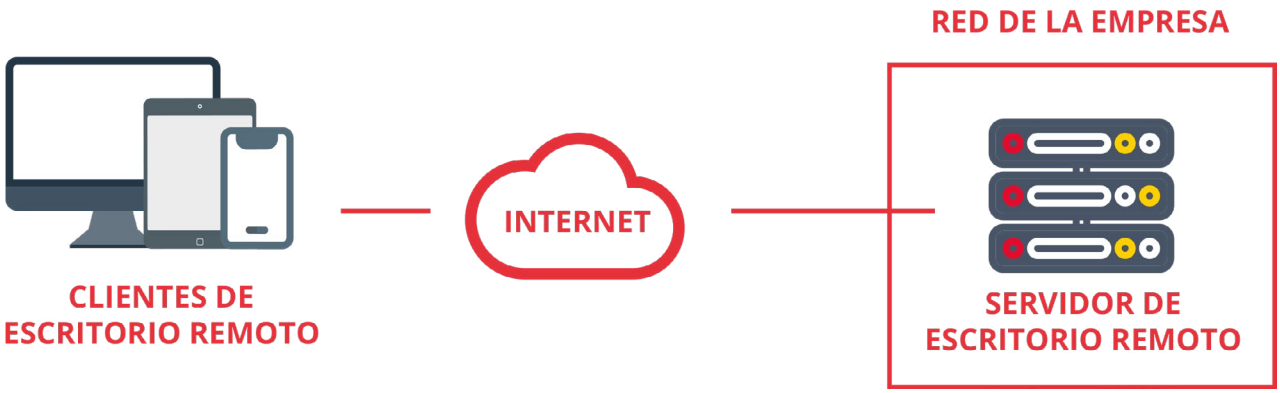


Ilustración 6: Modelo de acceso remoto

En este modelo de conexión, el teletrabajador tiene control de teclado y ratón sobre el ordenador remoto y ve la pantalla de ese equipo en la pantalla del dispositivo con el que está trabajando. Uno de los escritorios remotos más conocido es RDP, ya que se encuentra integrado en el sistema operativo Windows, aunque existen otras muchas opciones **[REF - 10]** . El acceso remoto al escritorio permite al usuario acceder a todas las aplicaciones, datos y otros recursos como si utilizara su ordenador en la oficina. El funcionamiento se basa en que un programa cliente de acceso de escritorio remoto o *plug-in* de navegador web está instalado en cada dispositivo cliente de teletrabajo, y se conecta directamente con la correspondiente estación de trabajo interna del empleado en la red interna de la organización.

4

"Las aplicaciones de **acceso de escritorio remoto** proporcionan al teletrabajador la posibilidad de controlar remotamente un equipo, siendo habitual conectarse al equipo del que se es usuario en la oficina de la organización, desde un dispositivo cliente de teletrabajo."

A simple vista puede parecer un buen método para conectarnos remotamente, ya que la instalación de estas aplicaciones es muy sencilla y no requiere de altos conocimientos técnicos para su implantación. La parte negativa es que estas herramientas pueden crear puertas traseras *(backdoors)* **[REF - 3]** a través de las cuales podría comprometerse el servicio o las credenciales de acceso de usuario y por lo tanto permitir el acceso a los equipos corporativos. Además, al usar este tipo de aplicaciones podemos estar aceptando ciertos términos y condiciones de uso que podrían otorgar algún tipo de privilegio a las mismas sobre nuestros equipos e información como por ejemplo la cesión de los datos recabados con fines comerciales. Recuerda leer siempre con atención «la letra pequeña» en concreto, los términos y condiciones y la política de privacidad, antes de implementar una solución de escritorio remoto.

Otro problema grave de seguridad con el *software* de escritorio remoto es que está descentralizado; es decir, en lugar de que la organización tenga que proteger un único servidor de puerta de enlace VPN, es necesario proteger cada estación de trabajo interna a la que se puede acceder a través del acceso de escritorio remoto. Debido a que se puede acceder a estas estaciones de trabajo internas desde Internet, por lo general necesitan estar protegidas con el mismo rigor que los servidores de acceso remoto. Elevar la seguridad a un nivel aceptable requeriría una cantidad significativa de tiempo y recursos, así como la implementación de controles de seguridad adicionales.
Si a pesar de no ser la opción más recomendada, optas por utilizar aplicaciones de escritorio remoto en tu organización, será necesario aplicar las siguientes recomendaciones de seguridad:

- Revisar que todo el *software* esté actualizado a la última versión y comprobar[10] que los equipos no están afectados por vulnerabilidades, como por ejemplo la Vulnerabilidad en el escritorio remoto de Windows de versiones antiguas.

10 Puedes estar al día de todas las novedades de seguridad para mantener tus sistemas seguros en la sección de Protege tu empresa: Avisos de seguridad

4

- No utilizar el puerto por defecto[11] (3389).
- Cambiar el usuario por defecto, nunca usar uno del tipo «admin», «administrador», etc.
- Utilizar siempre contraseñas robustas **[REF - 20]**.
- Implantar políticas de bloqueo de cuenta o *lock-out,* las cuales bloquean el acceso al servicio tras un número pre-establecido de intentos de autenticación fallidos.
- Aplicar el doble factor de autenticación siempre que sea posible **[REF - 17]**.
- Utilizar listas de control de acceso mediante NLA (por sus siglas en inglés *Network Level Authentication*). Mediante esta tecnología, los usuarios deben autenticarse en la red de la empresa antes de poder hacerlo en el servidor de escritorio remoto.
- Así mismo, es recomendable crear reglas específicas en el cortafuegos **[REF - 18]** de la empresa que restrinjan el acceso al servidor de escritorio remoto a un conjunto de máquinas controlado.

"Para evitar esta situación y ofrecer un extra de seguridad y privacidad a las comunicaciones, lo más recomendable es **utilizar a la vez una VPN y el escritorio remoto.** "

En general, habilitar el acceso al escritorio desde Internet no es recomendable, puesto que, en caso de existir una vulnerabilidad o configuración inadecuada, los ciberdelincuentes lo tendrán más fácil para entrar en la red corporativa. Para evitar esta situación y ofrecer un extra de seguridad y privacidad a las comunicaciones, lo más recomendable es **utilizar a la vez una VPN y el escritorio remoto**. Cuando un empleado desee acceder a su cuenta por medio del escritorio remoto, primero deberá acceder a la VPN, la cual proporcionará el acceso al escritorio remoto, así se contará con dos sistemas distintos que harán el sistema más robusto.

11 Comúnmente, la conexión al servicio de escritorio remoto de Windows se hace por medio del puerto 3389. Si se cambia por otro distinto, se dificultará los ataques automatizados que llevan a cabo los ciberdelincuentes. Esto se conoce como seguridad por oscuridad.

4

4.8. Soluciones en la nube

Las soluciones en la nube ofrecen gran versatilidad y un modelo diferente a la hora de compartir y almacenar información cuando teletrabajamos. Por este motivo, además de las implementaciones explicadas anteriormente contemplamos las distintas opciones a la hora de utilizar las soluciones en la nube para llevar a cabo las funciones diarias fuera de la oficina.

4.8.1. Portales para aplicaciones

Otra de las opciones para implementar soluciones de acceso remoto en la organización son los portales para aplicaciones. Un portal es un servidor[12] que proporciona el acceso a una o más aplicaciones corporativas a través de una interfaz única centralizada. La mayoría de estos portales están basados en web, por lo que el teletrabajador solo necesita utilizar un navegador como cliente para acceder a las aplicaciones de la empresa y poder realizar las funciones relativas a su trabajo. Cada empleado tendrá un perfil configurado en el que se le dará acceso solo a aquellas aplicaciones necesarias para desempeñar su trabajo.

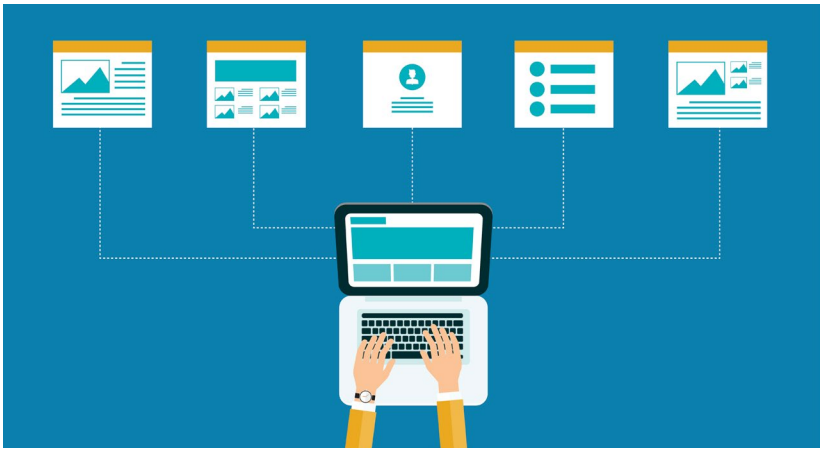
"Otra de las opciones para implementar soluciones de acceso remoto en la organización son los **portales para aplicaciones**. Un portal es un servidor que proporciona el acceso a una o más aplicaciones corporativas a través de una interfaz única centralizada. "

En términos de seguridad, los portales protegen la información que se intercambia entre los dispositivos cliente y el portal, proporcionando control de acceso y autenticación entre otros servicios de seguridad.

Los portales y las VPN comparten características de seguridad y se diferencian en la ubicación del *software* cliente de la aplicación y de los datos asociados. En la VPN, el *software* y los datos están en el dispositivo cliente y en un portal se encuentran en el servidor del portal, aunque estos se pueden configurar para permitir la descarga de contenido del portal y almacenarlo en el dispositivo cliente o en otros dispositivos fuera del entorno seguro.

12 Si el portal de aplicaciones está alojado en un servidor de la empresa este ya no sería considerado un servicio en la nube, si bien el concepto y la utilidad del portal de aplicaciones es el mismo.

4



En este caso debemos focalizar la seguridad en cada dispositivo que acceda al portal, ya que se trata de la puerta de entrada a la información de la organización. Es necesario recordar que las aplicaciones en la nube son aquellas provistas por un proveedor gratuitamente o a modo de suscripción, dejando en sus manos la disponibilidad, seguridad y soporte de las mismas así como la información que contienen **[REF - 21]**.

4.8.2. Herramientas colaborativas

Las tecnologías colaborativas **[REF - 22]** nos mantienen en contacto con nuestro equipo de trabajo cuando desempeñamos nuestras tareas fuera de la organización: paquetes ofimáticos, videoconferencias, pizarras virtuales, intercambio de documentos y ficheros, chats, etc.

Al utilizar estas herramientas debemos ser capaces de proporcionar la seguridad necesaria a la información que se intercambia y por ello establecer una serie de pautas básicas de seguridad, como las que exponemos a continuación.

- **Establecer comunicaciones solo con usuarios conocidos:** aunque parezca obvio, no se debe otorgar acceso a la red o establecer una comunicación con usuarios que no se encuentren dentro de nuestra lista de contactos. A la hora de poner en marcha un sistema de multiconferencia o videoconferencia, las medidas de seguridad deben girar en torno al control de accesos y a la protección de la información. Este tipo de medidas, que deben ser conocidas y acatadas por todos los empleados, son las mismas que se

"Las **tecnologías colaborativas** nos mantienen en contacto con nuestro equipo de trabajo cuando desempeñamos nuestras tareas fuera de la organización"

otorgarán a cualquier solicitud externa. Cabría la posibilidad de invitar a alguien cuyo sistema estuviera comprometido, lo que permitiría la propagación e infección a las distintas redes conectadas a través de este sistema de conferencia. En definitiva, deberemos usar el sentido común y únicamente permitir el acceso a aquellas solicitudes que sean de confianza y que únicamente accedan a la información que sea estrictamente necesaria para llevar a cabo el trabajo.

- **Prevenir la pérdida de datos y gestionar el almacenamiento:** una de las grandes ventajas de celebrar reuniones online o utilizar tecnologías de intercambio de información, es la capacidad de exponer en común y plantear nuevas ideas, sacar conclusiones o llegar a acuerdos. Será fundamental que la información surgida durante la reunión no se pierda cuando esta finalice. En la mayoría de las soluciones de videoconferencia y pantalla compartida, se ofrece algún tipo de capacidad de grabación de audio, visual o de texto. Estas grabaciones se almacenan en la nube, lo que aumenta el riesgo de pérdida de confidencialidad. Por lo tanto, cifrar este tipo datos será fundamental para preservar su integridad y confidencialidad.

- **Mantener la disponibilidad de la red:** las tecnologías colaborativas dependen de la conexión a Internet. Esta conexión deberá ser constante y confiable. Una pérdida de conexión hará que el intercambio de información no se pueda llevar a la práctica. Para evitar este tipo de problemas, debemos asegurarnos de que la conexión de red cuente con el suficiente ancho de banda para asegurar su funcionamiento óptimo. Además, también deberán funcionar otro tipo de herramientas, como los antivirus o los cortafuegos, ya que serán nuestra principal defensa ante ataques de código malicioso, denegación de servicio entre otras amenazas.

- **Integración con el resto de tecnologías:** este tipo de herramientas deberá integrarse con el resto de tecnologías TI de la organización, evitando problemas derivados de la incompatibilidad de sistemas o con las medidas de seguridad. La aparición de los servicios en la nube ha simplificado mucho este proceso eliminando gran parte de la molestia que podría ocasionar la administración de *hardware*.

4

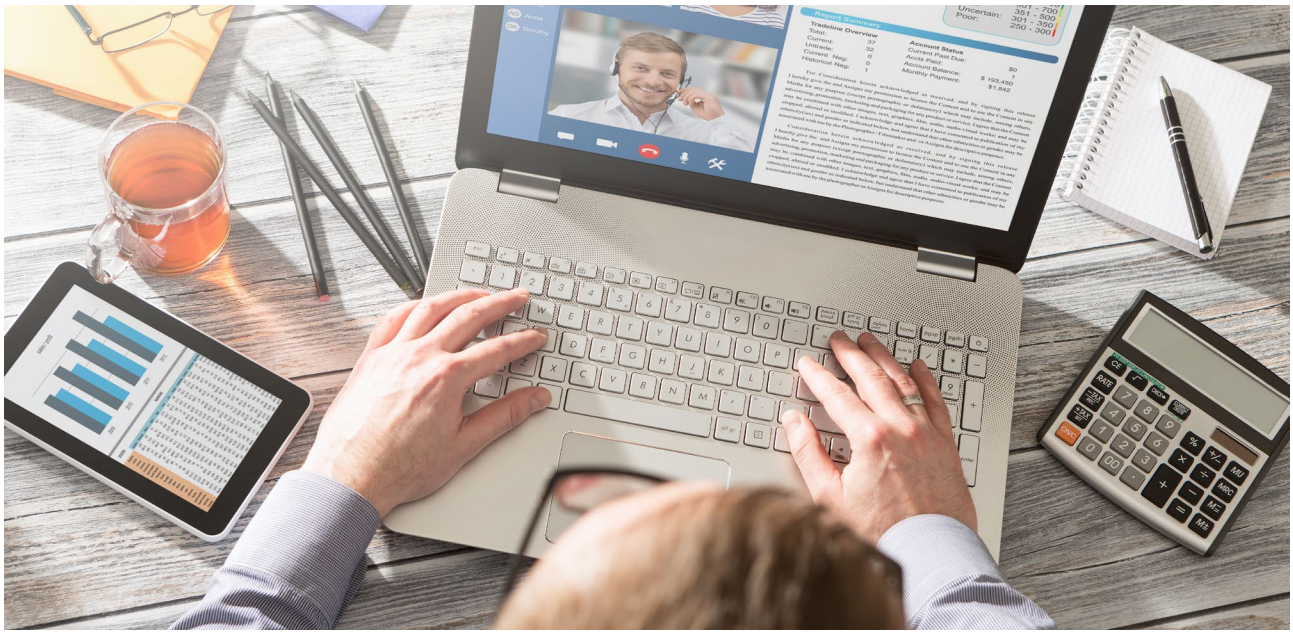
4.8.3. Recomendaciones de seguridad en el uso de aplicaciones de videollamada

Las aplicaciones de videollamada son herramientas fundamentales para mantener el contacto directo del equipo de trabajo. Puesto que existe una amplia variedad de estas aplicaciones nos centraremos en las pautas generales de seguridad a la hora de utilizar estas herramientas.

- **Utilizar un plan empresarial en lugar de uno básico:** si utilizamos planes básicos o gratuitos de las herramientas colaborativas, no podremos aplicar todas las opciones para mejorar la seguridad de la aplicación ya que estarán limitadas. Por ello, siempre es recomendable decantarse por un plan empresarial verificando que cuenta con las medidas necesarias para hacer un uso seguro.

- **Activar la sala de espera y bloquear la reunión:** esta funcionalidad añade a los participantes de una conferencia en un entorno previo a la reunión, así el administrador de la sala puede comprobar si los asistentes son solo los permitidos. Desde esta sala de espera, verificando la identidad de cada participante invitado, les dará paso a la reunión o se la denegará si no está autorizado. Una vez que todos se hayan incorporado a la llamada, se bloqueará el acceso a nuevos participantes.

"Las aplicaciones de **videollamada son herramientas fundamentales** para mantener el contacto directo del equipo de trabajo. "



4

- **Requerir contraseña para acceder a la reunión:** muchas aplicaciones de videollamada cuentan con esta configuración habilitada por defecto. Verifícalo para forzar su uso en caso de que esté deshabilitada. Utiliza siempre una contraseña robusta **[REF - 20]** para evitar accesos de terceros no autorizados.

- **Poner atención al enviar la convocatoria:** es necesario compartir el enlace para que los participantes se puedan unir a la videollamada. Para ello, es recomendable utilizar las funciones de compartición de las propias aplicaciones y evitar el uso de redes sociales o canales de comunicación inseguros para lanzar la convocatoria.

- **Video y micrófono apagados por defecto:** algunas funciones por defecto, como la cámara o el micrófono activados, pueden dar lugar a situaciones poco deseables. Además, los participantes que se unan a una videollamada tampoco deben compartir su escritorio de forma predeterminada ya que esto podría provocar fugas de información. El administrador será quien permita que los usuarios muestren su escritorio cuando sea preciso.

  La recepción de video permanecerá deshabilitada por defecto y solo se utilizará cuando sea necesario. De esta forma se evitan posibles fugas de información y se reduce el consumo de ancho de banda. El micrófono también permanecerá apagado cuando no sea necesario su uso.

  Así mismo, conviene recordar que cuando compartimos nuestra pantalla con el resto de usuarios de la reunión se debe evitar compartir información confidencial, como: nombres de usuario o nombre de dispositivo, documentos confidenciales, nombres de archivos o directorios sensibles y direcciones web del navegador.

  Si el administrador pretende grabar la reunión, se lo comunicará previamente a todos los participantes.

4

- ***Software* oficial y actualizado:** las herramientas deben descargarse siempre desde la web oficial del desarrollador o desde repositorios oficiales. Nunca se descargará de enlaces obtenidos en medios como el correo electrónico, aplicaciones de mensajería instantánea o redes sociales, ya que puede dirigir a sitios web fraudulentos.

  Estas herramientas siempre estarán actualizadas a la última versión disponible y si fuera posible se marcará la opción de actualizaciones automáticas o que la aplicación avise al usuario en caso de existir una nueva actualización.

- **Conocer la política de privacidad de la herramienta:** antes de decantarse por una herramienta de videoconferencia, se debe conocer la política de privacidad que sigue el proveedor, para saber qué tratamiento realiza sobre la información confidencial. Algunas herramientas pueden seguir políticas cuya protección para los clientes no es tan robusta como la que requiere el cumplimiento del RGPD **[REF - 23]**, por lo que siempre hay que saber cómo actúan sobre los datos tratados.

- **Cifrado de las comunicaciones:** esta será una de las medidas de seguridad imprescindibles con las que debe contar la aplicación para asegurar que las comunicaciones no puedan ser espiadas por un tercero. Generalmente todas las principales aplicaciones cuentan con mecanismos de cifrado pero es conveniente comprobarlo antes de utilizarla.

5 SEGURIDAD DEL SERVIDOR DE ACCESO REMOTO

Habitualmente, cuando teletrabajamos necesitamos acceder a los recursos corporativos para desempeñar nuestro trabajo diario sin ningún tipo de restricción. Son los servidores de acceso remoto los que permiten que los dispositivos externos puedan acceder a los recursos internos, así como proporcionar un entorno de teletrabajo seguro y aislado. Un servidor comprometido podría permitir el acceso no autorizado a los recursos de la empresa y a los dispositivos cliente de teletrabajo para obtener información confidencial. Al implantar medidas de seguridad en estos servidores protegemos la información corporativa y por ende la continuidad de negocio.

Los servidores de acceso remoto deben mantenerse actualizados, utilizar una configuración de seguridad definida por la organización y deben ser gestionados únicamente por administradores autorizados. Se debe evaluar cuidadosamente la seguridad de cualquier solución que se ejecute en el servidor de acceso remoto ya que una vulnerabilidad en cualquiera de estas aplicaciones puede comprometer todo el servidor de acceso remoto, con los peligros que eso conlleva. Sin duda, la mejor práctica para garantizar la seguridad es tener el servidor de acceso remoto dedicado solo para este servicio.

5.1. Dónde colocar el servidor de acceso remoto

Los servidores de acceso remoto suelen estar situados en el perímetro de la red de la organización. Esta colocación es la más común porque las políticas de seguridad de la empresa se suelen aplicar a toda la red corporativa. Incluso si una política de seguridad particular se aplica a una subred de la organización, la mayoría de los servidores de acceso remoto pueden restringir el acceso a las subredes y, por lo tanto, pueden colocarse en el perímetro de la organización.

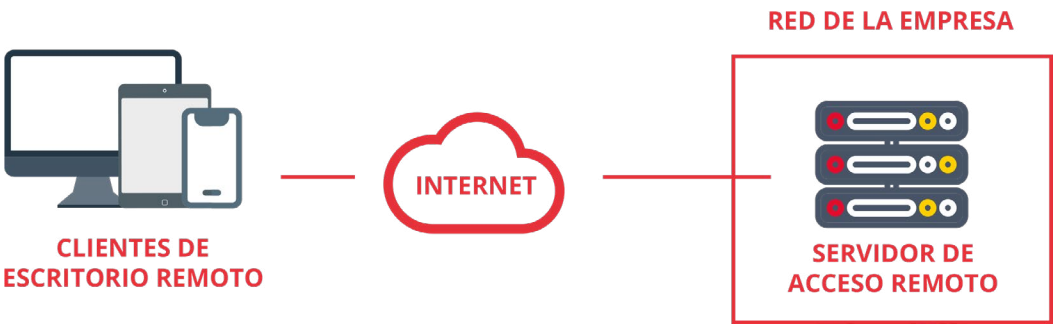


Ilustración 7: Servidor de acceso remoto en la red corporativa

5

5.2. Autenticación, autorización y control de acceso remoto

Los recursos informáticos accesibles mediante conexión remota solo deberían estar disponibles para los usuarios que realmente los usan y necesitan y no de forma generalizada. Para asegurar que el acceso está restringido adecuadamente, los servidores de acceso remoto deben verificar a cada teletrabajador antes de conceder cualquier acceso a los recursos e información de la organización así como utilizar tecnologías de autorización para asegurar que sólo se puedan utilizar los recursos necesarios que han de ser aprobados previamente para cada usuario. Además, tener contraseñas para los distintos servicios, reduce el impacto en otros recursos en caso de que alguna de estas contraseñas se viera comprometida.

> "Los recursos informáticos accesibles mediante conexión remota solo deberían estar disponibles para los **usuarios que realmente los usan y necesitan** y no de forma generalizada. "

Siempre que sea posible, la organización debe implementar la autenticación mutua, que permita a los usuarios remotos verificar la legitimidad del servidor antes de introducir sus credenciales, por ejemplo utilizando un certificado digital presentado por el servidor y así garantice su legitimidad. Algunos métodos de acceso remoto **[REF - 11]**, incluyen la autenticación obligatoria del servidor durante la configuración del canal de comunicaciones seguras.

Después de verificar la identidad de un usuario remoto se pueden realizar comprobaciones en el dispositivo cliente de teletrabajo para determinar a qué recursos internos debe permitirse el acceso a los usuarios. Estos controles se suelen denominan **controles de salud, idoneidad, detección o evaluación.** En estos controles, el servidor de acceso remoto comprueba en el dispositivo cliente distintos aspectos como: que cumpla la configuración de seguridad de la organización, que el antivirus este actualizado, que el sistema operativo esté correctamente parcheado, etc. También se pueden emitir certificados digitales a los dispositivos cliente para que se autentiquen como parte de estas comprobaciones.

6 SEGURIDAD DEL *SOFTWARE* CLIENTE DE ACCESO REMOTO

Otro aspecto importante a la hora de garantizar la seguridad de nuestras conexiones remotas es la configuración del *software* de acceso remoto. Muchos de estos clientes tienen características y configuraciones de seguridad que pueden ser configuradas remotamente por un administrador de sistemas, por lo que se recomienda que esta tarea sea realizada por el personal técnico y no por el usuario del *software* cliente. Si no se protegen adecuadamente, un posible atacante podría utilizar las capacidades de gestión remota para obtener acceso a los recursos internos de la organización. Además, para asegurar que la gestión remota está debidamente protegida se deben cifrar las comunicaciones de red y realizar la autenticación mutua de los puntos finales.

Las organizaciones deben planificar cómo se gestionarán los dispositivos cliente de teletrabajo que proporcionan a los teletrabajadores, como por ejemplo personal del servicio de asistencia técnica que acceda de forma remota a un dispositivo para realizar la resolución de los problemas que se reporten.

7 PRINCIPALES AMENAZAS PARA LOS TERMINALES DE TELETRABAJO

Permitir a los teletrabajadores acceder de forma remota a los recursos de la organización ofrece a los ciberdelincuentes oportunidades adicionales para vulnerar la seguridad de la empresa. Si los dispositivos no están correctamente protegidos supone un riesgo adicional no sólo para la información a la que accede el teletrabajador, sino también para los demás sistemas y redes de la organización.

Actualmente existen muchas amenazas que afectan a la seguridad de los dispositivos cliente de teletrabajo. Estas amenazas materializadas por ciberdelincuentes tienen diferentes motivaciones, incluyendo causar daño material y reputacional a la organización, robar propiedad intelectual, cometer robo de identidad y otras formas de fraude.

La principal amenaza contra la mayoría de los dispositivos cliente de teletrabajo es el *malware*, incluyendo virus, gusanos, troyanos, *rootkits*, *spyware* y *bots* **[REF - 3]**. Las amenazas de *malware* pueden infectar los dispositivos cliente a través de muchos medios, como el correo electrónico, los sitios web, las descargas y el uso compartido de archivos, la mensajería instantánea y las redes sociales. El uso de medios o dispositivos extraíbles no autorizados, como las memorias *flash*, es otro mecanismo muy común de transmisión del *malware*. Además de las anteriores, otra amenaza a destacar contra los dispositivos cliente de teletrabajo es la pérdida o el robo del dispositivo, ya que alguien con acceso físico a un dispositivo tiene muchas opciones para intentar ver o copiar la información almacenada en él. Un atacante con acceso físico también podría infectar con ***malware*** el dispositivo y así conseguir que le proporcione acceso a los datos a los que se accede o se introducen en dicho dispositivo, como por ejemplo las contraseñas de los usuarios que se escriben en el teclado de un ordenador portátil (*keylogger*).

Generalmente, los terminales de teletrabajo deben tener los mismos controles de seguridad que los que están físicamente en la empresa: aplicar las actualizaciones de seguridad, servicios innecesarios desactivados, etc. Sin embargo, debido a las amenazas a las que se enfrentan los dispositivos cliente en entornos externos, se recomiendan controles de seguridad adicionales, pudiendo ser necesario ajustar algunos controles de seguridad para que funcionen eficazmente en entornos de teletrabajo. En el siguiente apartado se exponen las recomendaciones para asegurar los terminales de teletrabajo y los datos que contienen.

7

Si el uso de controles de seguridad adicionales instalados en los dispositivos de teletrabajo no es factible o aplicable, se pueden estudiar otras medidas como proporcionar un entorno seguro para el teletrabajo a través del uso de tecnologías VDI o VMI, es decir, proporcionar a los teletrabajadores dispositivos previamente configurados para que puedan arrancar su equipo de teletrabajo en un entorno seguro, o adoptar soluciones de gestión de dispositivos móviles (*Mobile Device Management,* MDM) y de gestión de aplicaciones móviles (*Mobile Application Management,* MAM) para la mejora y aplicación de la seguridad en los dispositivos móviles.

Las organizaciones deberían ser responsables de asegurar sus propios dispositivos cliente de teletrabajo y también deberían exigir a sus usuarios que mantengan niveles de seguridad apropiados. Es importante que los empleados conozcan cómo se protege su puesto de trabajo **[REF - 24]**.

"La principal amenaza contra la mayoría de los dispositivos cliente de teletrabajo es el ***malware***, incluyendo virus, gusanos, troyanos, *rootkits*, *spyware* y *bots* **"**

8 ASEGURAR LOS EQUIPOS DE TRABAJO

Una de las consideraciones más importantes para los equipos de teletrabajo es la aplicación de actualizaciones de seguridad de sistemas operativos y aplicaciones. Por lo general todas las aplicaciones tienen que estar actualizadas, siendo las más críticas las que se utilizan por motivos de seguridad (por ejemplo, *software* anti*malware*, cortafuegos) o las de acceso remoto, y las que son objetivos frecuentes de ataques como navegadores web, clientes de correo electrónico y clientes de mensajería instantánea. Para los equipos de teletrabajo administrados por sus usuarios (dispositivos personales **[REF - 25]**), la mejor opción será activar las actualizaciones automáticas.

Las organizaciones deben contar con una política de actualizaciones de los equipos de teletrabajo **[REF - 26]**. Las organizaciones también deberían animar a los usuarios a actualizar completamente sus equipos de teletrabajo antes de llevarlos de viaje o a otros entornos no controlados y por tanto menos seguros.

Otras medidas de seguridad que son particularmente importantes para el teletrabajo incluyen las siguientes:

- Tener cuentas de usuarios separadas con privilegios limitados y adecuados para cada perfil de usuario que vaya a usar el equipo de teletrabajo. Esto reduce la probabilidad de que un ciberdelicuente obtenga un acceso con privilegios al equipo.

- Configurar el bloqueo de sesión que impida el acceso al equipo después de haber estado inactivo durante un período de tiempo (por ejemplo, 5 minutos). Esto impediría que un delincuente con acceso físico al equipo pudiera acceder fácilmente a la sesión actual en un descuido del usuario. Sin embargo, esta medida no frustra a un atacante que roba un PC o tiene acceso a él durante un período de tiempo prolongado; ya que el bloqueo de sesión se puede eludir mediante diversas técnicas.

- Proteger físicamente los equipos de teletrabajo mediante el uso de cerraduras de cable u otros elementos disuasorios contra el robo. Esto es lo más importante para los equipos de teletrabajo en entornos externos no confiables.

8

"Una de las consideraciones más importantes para los equipos de teletrabajo es la aplicación de actualizaciones de seguridad de sistemas operativos y aplicaciones."

- Existen soluciones que proporcionan un sistema operativo de inicio en un medio extraíble de sólo lectura con *software* cliente de acceso remoto preconfigurado. En la mayoría de los casos, estas soluciones pueden configurarse para evitar que los usuarios almacenen archivos en el disco duro local, guarden los archivos en medios extraíbles y transfieran información desde el sistema operativo conocido a otra ubicación. Las soluciones de sistemas operativos de arranque hacen que la seguridad lógica del PC de teletrabajo sea mucho menos importante, aunque no son la solución a todos los problemas de seguridad (por ejemplo, podría existir alguna vulnerabilidad en el sistema operativo del medio extraíble).

- Cifra tus soportes **[REF - 29]** de información para proteger los datos de tu empresa de posibles accesos malintencionados y garantizar así su confidencialidad e integridad.

9 ASEGURAR LOS DISPOSITIVOS MÓVILES DE TELETRABAJO

Los dispositivos móviles, incluidos los que se usan simultáneamente de manera personal y profesional (BYOD), deben estar contemplados en las políticas de seguridad de la empresa, ya que existen riesgos inherentes a su uso como el robo o pérdida, infección por *malware*, accesos no autorizados a recursos de la empresa o fugas de información. Si no existen estas políticas o no contemplan los usos permitidos de los móviles, estaremos expuestos a sufrir incidentes de seguridad.

Para la elaboración de estas políticas podemos utilizar las soluciones de gestión de dispositivos móviles (MDM) y las soluciones de gestión de aplicaciones móviles (MAM) diseñadas para controlar el uso de dispositivos móviles.

Podemos utilizar las soluciones MDM para aplicar las políticas de seguridad que consideremos necesarias. Por ejemplo, podríamos utilizar este *software* para requerir el uso de un PIN para desbloquear un dispositivo móvil, permitir que las tecnologías de cifrado protejan los datos confidenciales almacenados, así como determinar si un dispositivo móvil ha sufrido modificaciones de *software* para evadir las restricciones del fabricante (comúnmente conocido como *rootear* en el caso de los móviles Android o *jailbreak* en el caso de los iPhone).

El *software* de gestión de dispositivos móviles también se puede utilizar para realizar un borrado remoto cuando un dispositivo móvil se ha perdido o ha sido robado y así evitar el acceso no autorizado a cualquier dato confidencial que contenga. Una organización puede establecer diferentes políticas de gestión de dispositivos móviles para cada categoría, como por ejemplo, los emitidos por la organización, controlados por terceros y BYOD, y así tener en cuenta todos los diferentes niveles de acceso. Además proporciona un entorno que aísla las aplicaciones y los datos de la empresa del resto del dispositivo pudiéndose requerir una autenticación robusta para acceder al entorno empresarial, que a su vez está cifrado para proteger los datos y aplicaciones confidenciales de la organización, y para minimizar la fuga de datos de esas aplicaciones a otras aplicaciones y servicios que se ejecutan en el dispositivo.

En el caso de que el dispositivo se pierda o el empleado abandone la organiza-

9

"Los dispositivos móviles, incluidos los que se usan simultáneamente de manera personal y profesional (BYOD), deben estar contemplados en las **políticas de seguridad de la empresa**."

ción, el entorno protegido puede borrarse de forma remota para eliminar los datos de la empresa.

La opción más completa para mantener la seguridad de estos dispositivos es el *software* conocido como UEM, **[REF - 27]** por sus siglas en inglés *Unified Endpoint Management*, que permite administrar de forma centralizada todos los dispositivos de la empresa de manera remota. Esta herramienta aúna las características de la gestión de dispositivos móviles o MDM anteriormente descritos y la gestión de movilidad empresarial EMM *(Enterprise Mobility Management)*, simplificando así el coste en tiempo y recursos en las labores de administración. Los UEM, además de permitir a la empresa gestionar los dispositivos móviles, proporcionan las herramientas necesarias para administrar otros elementos corporativos como impresoras, dispositivos IoT **[REF - 28]** o equipos de sobremesa.

Las organizaciones pueden aprovechar estas capacidades de gestión de la seguridad, por ejemplo, restringiendo la instalación y el uso de aplicaciones de terceros, o proporcionando una serie de aplicaciones autorizadas. No obstante, las capacidades de seguridad y las acciones apropiadas varían ampliamente según el tipo de dispositivo, las aplicaciones que necesite tener instaladas y los permisos solicitados por estas. Por ello, las organizaciones deben proporcionar a los administradores de dispositivos y a los usuarios las pautas necesarias para protegerlos, ya que ambos, administradores y usuarios, son responsables de la seguridad de los dispositivos móviles de teletrabajo **[REF - 30]**.

Entre los consejos de seguridad generales para dispositivos móviles destacamos:

- Limitar las capacidades de red, como por ejemplo el uso del Bluetooth y redes inalámbricas compartidas, priorizando en estos casos el uso de la redes móviles (3G/4G/5G). Existe la posibilidad de que algunos protocolos inalámbricos expongan al dispositivo a un posible ataque por parte de los ciberdelincuentes.

- Los dispositivos que se conectan a Internet deben disponer de *software antimalware* e incluso de cortafuegos habi-

9

litados para evitar ataques y accesos no autorizados.

- Aplicar las actualizaciones y parches del fabricante cuando sea necesario para proteger el dispositivo de los ataques que explotan vulnerabilidades conocidas y no parcheadas.
- Cifrar los datos almacenados en el dispositivo.
- Requerir autenticación antes de acceder a los recursos de la organización.
- Restringir las aplicaciones que pueden o no instalarse mediante listas blancas o negras.
- Dada la similitud entre las funciones de los dispositivos móviles, especialmente a medida que aumentan sus capacidades y las de los equipos de sobremesa o portátiles, las organizaciones deberían considerar aumentar las medidas de seguridad hasta equipararlas con las de los equipos que se utilizan en las instalaciones de la empresa.

10 PROTECCIÓN DE DATOS EN TERMINALES DE TELETRABAJO

El teletrabajo suele implicar la creación y modificación de información en función de la actividad diaria como por ejemplo el manejo del correo electrónico, documentos de texto y hojas de cálculo, etc. Debido a que esos documentos pueden contener datos sensibles de la organización, deben ser tratados con la seguridad que requieren. Las dos medidas principales que se pueden tomar para proteger los datos en los dispositivos de teletrabajo son asegurarlos en el propio dispositivo de teletrabajo y realizar copias de seguridad periódicas en una ubicación controlada por la empresa. Adicionalmente, se podría contemplar la opción de no permitir que la información se almacene en dispositivos de teletrabajo, sino almacenarla de forma centralizada en la organización.

Información sensible, como por ejemplo registros de personal, registros médicos o registros financieros, que se almacenan o se envían a o desde dispositivos de teletrabajo, debe ser protegida para que no sea accesible ni modificable. Los teletrabajadores a menudo olvidan que almacenar información sensible en un dispositivo externo, o imprimir esta información en una impresora pública, también puede poner en peligro su confidencialidad. Una divulgación no autorizada de información sensible podría además de tener consecuencias legales **[REF -23]**, dañar la imagen de la organización y por consiguiente la confianza de los clientes hacia la misma.

En cualquier caso, las organizaciones deben proporcionar las medidas de seguridad a aplicar a los usuarios responsables de los dispositivos móviles de teletrabajo sobre cómo deben protegerlos. Consulta estas dos políticas de seguridad para ampliar la información:

- Política de uso de dispositivos móviles corporativos **[REF - 30]**.
- Políticas de uso de dispositivos móviles no corporativos **[REF - 25]**.

11 COPIA DE SEGURIDAD DE DATOS EN DISPOSITIVOS DE TELETRABAJO

La mayoría de las organizaciones poseen políticas para realizar copias de seguridad de los datos de forma regular. Esta política de copias de seguridad debe contemplar también los datos de los equipos de teletrabajo y de los dispositivos móviles asignados a esta tarea. Sin embargo, una política de este tipo puede necesitar disposiciones diferentes para las copias de seguridad realizadas en las instalaciones de la organización en comparación con las ubicaciones externas.

Si los datos de los que se va a realizar la copia de seguridad contienen información confidencial o necesitan que se proteja su confidencialidad por otras razones, existen consideraciones de seguridad adicionales si la copia de seguridad se realiza en una ubicación externa.

En el caso de que los datos estén siendo respaldados remotamente desde el dispositivo de teletrabajo hasta un sistema de la organización, las comunicaciones que transportan esos datos deben ser cifradas y así garantizar su integridad. Si se están haciendo copias de seguridad de los datos localmente (por ejemplo, en medios extraíbles, discos duros externos o unidades *flash*), la copia de seguridad debe estar protegida con la misma rigurosidad que los datos originales, es decir, si los datos originales están cifrados, entonces los datos de la copia de seguridad también deberían estar cifrados.

Consulta nuestra guía «Copias de seguridad: una guía de aproximación para el empresario» **[REF - 31]** para conocer todas las medidas referentes a las copias de seguridad en el entorno empresarial.

12 RESUMEN

Después de leer esta guía seguro que tienes más claro por qué es necesario tener en cuenta las medidas de seguridad a la hora de teletrabajar. A modo de resumen, consulta este apartado siempre que necesites recordar los pasos más importantes a la hora de trabajar fuera de la organización.

- **Red privada virtual o VPN:** conéctate a través de una VPN para evitar que los ciberdelincuentes puedan espiar tus comunicaciones.
- **VPN + escritorio remoto:** evita riesgos derivados de las vulnerabilidades o configuraciones inadecuadas. Si utilizas el escritorio remoto, que sea a través de VPN.
- **Dispositivos corporativos la mejor opción:** cuentan con las políticas de seguridad que la empresa estima oportunas y tienen instalado el *software* necesario para realizar el trabajo.
- **Dispositivos personales:** siempre bajo una política BYOD.
- **Crea un entorno de trabajo seguro:** tanto en tu casa como en tu oficina respeta la política de protección del puesto de trabajo.
- **Protege tu conexión a Internet:** se utilizará preferiblemente la red doméstica, y se evitará utilizar redes wifi públicas. **[REF - 32]**
- **Red de datos móvil como plan B:** Cuando no sea posible utilizar la red doméstica para teletrabajar o cualquier otra red considerada segura como alternativa, utiliza la red de datos móvil 4G o 5G.
- **Periodo de implantación y pruebas:** valora diferentes escenarios y configuraciones antes de comenzar a teletrabajar.
- **Elabora una política de teletrabajo:** y forma a tus empleados para que puedan seguirla.

13 REFERENCIAS

[REF - 1]. **Incibe, Políticas de seguridad para la pyme – Almacenamiento en los equipos de trabajo** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/almacenamiento-en-los-equipos-trabajo.pdf

[REF - 2]. I**ncibe, Políticas de seguridad para la pyme – Almacenamiento en la red corporativa** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/almacenamiento-red-corporativa.pdf

[REF - 3]. **Incibe, Glosario de términos de ciberseguridad: una guía de aproximación para el empresario** https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario

[REF - 4]. **Incibe, Cómo prevenir incidentes en los que intervienen dispositivos móviles** https://www.incibe.es/protege-tu-empresa/blog/prevenir-incidentes-los-intervienen-dispositivos-moviles

[REF - 5]. **Incibe, kit de concienciación** https://www.incibe.es/protege-tu-empresa/kit-concienciacion

[REF - 6]. **Incibe, Leyes en ciberseguridad que afectan a tu empresa** https://www.incibe.es/protege-tu-empresa/blog/leyes-ciberseguridad-afectan-tu-empresa

[REF - 7]. **Incibe, Protección de la información** https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion

[REF - 8]. **Incibe, Políticas de seguridad para la pyme** – Uso de técnicas criptográficas https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-_tecnicas-criptograficas.pdf

[REF - 9]. **Incibe, Avisos de seguridad** https://www.incibe.es/protege-tu-empresa/avisos-seguridad

[REF - 10]. **Incibe, Catálogo de empresas y soluciones de Ciberseguridad** https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad

[REF - 11]. **vpnMentor - Diferentes tipos de VPN y cuándo usarlas** https://es.vpnmentor.com/blog/diferentes-tipos-de-vpn-y-cuando-usarlas/

13

[REF - 12]. **vpnMentor - ¿Qué protocolo VPN debería utilizar?** https://es.vpnmentor.com/blog/que-protocolo-vpn-deberia-utilizar/

[REF - 13]. **Incibe, Sistemas VDI y teletrabajo, la dupla perfecta en tiempos del COVID-19** https://www.incibe.es/protege-tu-empresa/blog/sistemas-vdi-y-teletrabajo-dupla-perfecta-tiempos-del-covid-19

[REF - 14]. **Incibe, Contratación de servicios** https://www.incibe.es/protege-tu-empresa/que-te-interesa/contratacion-servicios

[REF - 15]. **Incibe, Políticas de seguridad para la pyme** https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[REF - 16]. **Incibe, Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario** https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf

[REF - 17]. **Incibe, Dos mejor que uno: doble factor para acceder a servicios críticos** https://www.incibe.es/protege-tu-empresa/blog/dos-mejor-uno-doble-factor-acceder-servicios-criticos

[REF - 18]. **Incibe, Firewall tradicional, UTM o NGFW. Diferencias, similitudes y cuál elegir según tus necesidades** https://www.incibe.es/protege-tu-empresa/blog/firewall-tradicional-utm-o-ngfw-diferencias-similitudes-y-cual-elegir-segun

[REF - 19]. **Incibe, ¿Es seguro tu escritorio remoto?** https://www.incibe.es/protege-tu-empresa/blog/seguro-tu-escritorio-remoto

[REF - 20]. **Incibe, Desempolvando Políticas de seguridad: las contraseñas** https://www.incibe.es/protege-tu-empresa/blog/desempolvando-politicas-seguridad-las-contrasenas

[REF - 21]. **Incibe, Protege tu información, aplica estas recomendaciones de seguridad en servicios de almacenamiento cloud** https://www.incibe.es/protege-tu-empresa/blog/protege-tu-informacion-aplica-estas-recomendaciones-seguridad-servicios

[REF - 22]. **Incibe, Herramientas colaborativas: medidas básicas de seguridad** https://www.incibe.es/protege-tu-empresa/blog/herramientas-colaborativas-medidas-basicas-seguridad

[REF - 23]. **Incibe, Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario** https://www.incibe.es/protege-tu-empresa/guias/ganar-competitividad-cumpliendo-el-rgpd-guia-aproximacion-el-empresario

[REF - 24]. **Incibe, Políticas de seguridad para la pyme – Protección del puesto de trabajo** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/proteccion-puesto-trabajo.pdf

[REF - 25]. **Incibe, Políticas de seguridad para la pyme – Uso de dispositivos móviles no corporativos** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-dispositivos-moviles-no-corporativos.pdf

[REF - 26]. **Incibe, Políticas de seguridad para la pyme – Actualizaciones de *software*** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/actualizaciones-*software*.pdf

[REF - 27]. **Incibe, Cómo prevenir incidentes en los que intervienen dispositivos móviles** https://www.incibe.es/protege-tu-empresa/blog/prevenir-incidentes-los-intervienen-dispositivos-moviles

[REF - 28]. **Incibe, Seguridad en la instalación y uso de dispositivos IoT: una guía de aproximación para el empresario** https://www.incibe.es/protege-tu-empresa/guias/seguridad-instalacion-y-uso-dispositivos-iot-guia-aproximacion-el

[REF - 29]. I**ncibe, Uso de técnicas criptográficas** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-_tecnicas-criptograficas.pdf

[REF - 30]. I**ncibe, Políticas de seguridad para la pyme – Uso de dispositivos móviles corporativos** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-dispositivos-moviles-corporativos.pdf

[REF - 31]. **Incibe, Copias de seguridad: una guía de aproximación para el empresario** https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

[REF - 32]. **Incibe, Seguridad en redes wifi: una guía de aproximación para el empresario** Seguridad en redes wifi: una guía de aproximación para el empresario

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa

I. COMUNIDAD DE CASTILLA Y LEÓN

A. DISPOSICIONES GENERALES

CONSEJERÍA DE LA PRESIDENCIA

DECRETO 16/2018, de 7 de junio, por el que se regula la modalidad de prestación de servicios en régimen de teletrabajo en la Administración de la Comunidad de Castilla y León.

El Estatuto de Autonomía de Castilla y León establece en el artículo 32.3 que en el ejercicio de la competencia de organización, régimen y funcionamiento, prevista en el artículo 70.1.1º, y de acuerdo con la legislación del Estado, corresponde a la Comunidad Autónoma el establecimiento del régimen de los empleados públicos de su Comunidad.

El texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por el Real Decreto Legislativo 5/2015, de 30 de octubre, señala que las Administraciones Públicas establecerán la jornada de trabajo de sus funcionarios públicos y que en relación con el régimen de jornada de trabajo del personal laboral se estará a lo establecido en este capítulo y en la legislación laboral correspondiente, siendo el artículo 13 del texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, el que regula el trabajo a distancia.

La Ley 7/2005, de 24 de mayo, de la Función Pública de Castilla y León en su artículo 104, establece entre las materias objeto de negociación las que afecten a las condiciones de trabajo de los empleados públicos.

El Acuerdo Marco de 29 de octubre de 2015 entre la Administración de la Comunidad de Castilla y León y las organizaciones sindicales CSI-F, UGT y CCOO por el que se recuperan derechos de los empleados públicos y se fijan prioridades en materia de función pública para la Legislatura 2015/2019, recoge expresamente dentro de las medidas destinadas a mejorar y modernizar la función pública de Castilla y León, la evaluación del teletrabajo y la adopción de las decisiones oportunas para su optimización.

La disposición que actualmente regula el teletrabajo es el Decreto 9/2011, de 17 de marzo, por el que se regula la jornada de trabajo no presencial mediante teletrabajo en la Administración de Castilla y León, cuyo objetivo fundamental ha sido desvincular al empleado público del lugar físico de desempeño de su puesto de trabajo con la finalidad de dar un paso más en la conciliación de la vida familiar y laboral.

Los años de experiencia desde su implantación y la auditoría realizada por Inspección General de Servicios dentro de su Plan de actuación para el 2016, destinada a la «Evaluación de la prestación de servicios a la Administración en la modalidad de teletrabajo», han permitido analizar los puntos débiles de este sistema de trabajo, que exigen una nueva regulación para garantizar su eficacia.

La implantación de la administración electrónica hace previsible que los puestos susceptibles de ser ocupados en régimen de teletrabajo aumenten, en la medida que muchas de las funciones ligadas a la permanencia en el centro de trabajo podrán ser desempeñadas desde cualquier lugar en que existan los medios tecnológicos necesarios para su prestación.

En el marco descrito, el teletrabajo puede perseguir objetivos más ambiciosos que los existentes hasta ahora, ya que resulta un instrumento idóneo para contribuir a la organización de los recursos humanos al servicio de la Administración Pública, a la protección de la salud del personal a su servicio así como a la sostenibilidad del medio ambiente, por lo que se considera necesario llevar a cabo una nueva regulación que se adapte a las nuevas necesidades y a los avances que se han producido en estos últimos años.

El presente decreto se adecua a los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia exigidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Tanto el principio de necesidad como el de eficacia exigen que la norma sirva al interés general, que consiste en posibilitar el cumplimiento del mandato normativo de regular las condiciones de trabajo de los empleados públicos y el derecho a la adopción de medidas que favorezcan la conciliación de la vida personal, familiar y laboral.

Así, el decreto es necesario pues permite establecer los cauces procedimentales a través de los cuales ha de efectuarse la prestación de servicios en régimen de teletrabajo en la Administración de la Comunidad de Castilla y León, y la eficacia queda garantizada a través del establecimiento de un procedimiento ágil y que requiere el menor coste posible.

De acuerdo con el principio de proporcionalidad, la regulación que esta norma contiene es la imprescindible para atender a las exigencias que el interés general requiere. No supone restricción de derecho alguno y las obligaciones que impone a sus destinatarios son las indispensables para garantizar un procedimiento reglado y ordenado en la prestación de servicios en régimen de teletrabajo.

Para garantizar el principio de seguridad jurídica, el decreto se integra en un marco normativo estable y coherente, resultando su contenido acorde con la regulación sobre la materia establecida en el Texto Refundido de la Ley del Estatuto Básico del Empleado Público y en la Ley 7/2005, de 24 de mayo, de la Función Pública de Castilla y León.

Igualmente, la regulación contenida en la norma contribuye a hacer efectivo el principio de eficiencia, de forma que se consigue la realización efectiva de la modalidad de teletrabajo a través de los menores costes posibles y con los medios más adecuados.

Los principios de transparencia y participación han sido respetados en la tramitación de esta norma, pues se ha posibilitado a los ciudadanos la participación en la elaboración de su contenido a través de la plataforma de Gobierno Abierto y se han llevado a cabo todos los trámites establecidos tanto en la normativa estatal básica como autonómica relacionados con la participación de los ciudadanos en la determinación del contenido de la disposición.

El decreto se estructura en cinco capítulos, de los cuales el primero recoge las disposiciones generales que establecen el objeto, un conjunto de definiciones necesarias para hacer comprensivo el texto de la norma, los órganos competentes para su autorización,

el ámbito de aplicación y los requisitos necesarios para acceder a la modalidad de teletrabajo.

El capítulo segundo dedicado a la autorización de prestación de servicios en régimen de teletrabajo establece las características de dicha autorización, su duración, prórroga, suspensión, pérdida de efectos, renuncia y su extinción automática.

El capítulo tercero regula el régimen jurídico del personal que presta servicios en régimen de teletrabajo reconociéndole los mismos derechos y deberes que el resto del personal y estableciendo un conjunto de especialidades en distintas materias.

El capítulo cuarto establece las distintas fases del procedimiento para la autorización de prestación de servicios en régimen de teletrabajo y el capítulo quinto regula la comisión de seguimiento del teletrabajo.

La parte final se compone de una disposición transitoria en la que se establece el régimen de vigencia y validez de las autorizaciones existentes a la entrada en vigor del presente decreto y sus correspondientes prórrogas, una disposición derogatoria por la que se deroga expresamente el Decreto 9/2011, de 17 de marzo, y dos disposiciones finales. La primera habilita al Consejero competente en materia de Función Pública a dictar Órdenes en aplicación del Decreto y la segunda establece el día de su entrada en vigor.

Respecto a su tramitación, cumpliendo el artículo 133 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se ha realizado consulta pública previa.

Redactado el proyecto conforme a lo dispuesto en la Ley 3/2015, de 4 de marzo, de Transparencia y Participación Ciudadana se puso a disposición de todos los ciudadanos en el Portal del Gobierno Abierto de Castilla y León durante un plazo de diez días.

Se efectuó también el trámite de audiencia establecido en el artículo 133 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

El proyecto fue informado por todas las consejerías de acuerdo con lo establecido en los artículos 75 y 76 de la Ley 3/2001, de 3 de julio, del Gobierno y de la Administración de la Comunidad de Castilla y León.

De acuerdo con el artículo 76.2 de la Ley 2/2006, de 3 de mayo, de la Hacienda y del Sector Público de la Comunidad de Castilla y León, el estudio sobre su repercusión económica fue informado por la Consejería de Economía y Hacienda y el decreto ha sido informado también por los Servicios Jurídicos de la Comunidad.

Se han cumplido los trámites de negociación y de informe por los órganos competentes en materia de función pública, de acuerdo con lo establecido en la Ley 7/2005, de 24 de mayo, de la Función Pública de Castilla y León.

Dando cumplimiento a lo establecido en los artículos 75 y 76 de la Ley 3/2001, de 3 de julio, del Gobierno y de la Administración de la Comunidad de Castilla y León, el proyecto se ha sometido al dictamen del Consejo Consultivo de Castilla y León.

El Decreto 40/2015, de 23 de julio, por el que se establece la estructura orgánica de la Consejería de la Presidencia, atribuye a ésta las competencias en materia de función pública, que ejerce a través de la Viceconsejería de Función Pública y Gobierno Abierto.

La competencia de la Junta de Castilla y León para su aprobación se recoge en los artículos 6.1 y 6.2.r) de la Ley 7/2005, de 24 de mayo, de la Función Pública de Castilla y León.

En su virtud, la Junta de Castilla y León, a propuesta del Consejero de la Presidencia, de acuerdo con el dictamen del Consejo Consultivo de Castilla y León, y previa deliberación del Consejo de Gobierno en su reunión de 7 de junio de 2018

DISPONE

CAPÍTULO I

Disposiciones generales

Artículo 1. Objeto.

El presente decreto tiene por objeto regular la prestación de las funciones propias del puesto de trabajo fuera de las dependencias de la Administración de la Comunidad de Castilla y León a través de las nuevas tecnologías de la información y de la comunicación.

Artículo 2. Definiciones.

1. Teletrabajo.– Modalidad de prestación de servicios de carácter no presencial en virtud de la cual un trabajador puede desarrollar parte de las funciones propias de su puesto de trabajo desde su oficina a distancia mediante el uso de medios telemáticos. Esta modalidad de prestación de servicios tendrá carácter voluntario.

2. Teletrabajador.– Empleado público de la Administración de la Comunidad de Castilla y León que, en el desempeño de las funciones propias de su puesto de trabajo, alterna la presencia en el centro de trabajo con la prestación de servicios en régimen de teletrabajo.

3. Supervisor.– Empleado público que debe definir con el teletrabajador el documento de compromisos al que se refiere el apartado 8 de este artículo y realizar su seguimiento a través del plan individual de teletrabajo definido en el apartado 9. Será nombrado supervisor el encargado de dirigir, coordinar o controlar las funciones propias del puesto de trabajo que solicita ser desempeñado en régimen de teletrabajo.

4. Superior.– Empleado público con rango mínimo de Jefe de Servicio que ostenta la jefatura del solicitante de teletrabajo o del teletrabajador. El supervisor y el superior podrán ser la misma persona. En caso de que así sea, no se duplicarán los trámites en que hayan de intervenir ambos.

5. Oficina a distancia.– Lugar elegido por el solicitante de teletrabajo para desempeñar las jornadas no presenciales, que deberá disponer de los medios tecnológicos necesarios para realizar las funciones propias de su puesto de trabajo y en el que quedarán garantizadas las condiciones exigidas en materia de prevención de riesgos laborales, de privacidad y de confidencialidad de los datos.

6. Jornadas teletrabajables.– Son las jornadas en las que el teletrabajador desempeña sus funciones en la oficina a distancia. Su número se especificará en la solicitud y se determinará en el documento de compromisos al que se refiere el apartado 8. Éstas no podrán exceder de cuatro a la semana.

7. Períodos de interconexión.– Son los espacios de tiempo de trabajo efectivo durante los cuales el teletrabajador debe estar disponible para contactar con el supervisor así como con el resto de los miembros de la unidad o el órgano administrativo en el que preste funciones.

8. Documento de compromisos.– Es el instrumento en el que el teletrabajador formaliza las obligaciones que adquiere en relación con la prestación de servicios durante las jornadas teletrabajables.

Su contenido deberá ser establecido entre el supervisor y el teletrabajador y sometido posteriormente a informe favorable del superior.

La eficacia de la resolución de autorización del teletrabajo quedará vinculada al cumplimiento de su contenido y el documento de compromisos permanecerá vigente mientras lo esté dicha resolución.

Contendrá los siguientes extremos:

a) El nivel de teletrabajo al que se acoge el solicitante.

b) La ubicación de la oficina a distancia.

c) La determinación de los períodos de interconexión y de los medios para hacerlos efectivos.

d) La descripción de la forma de organización del trabajo así como el compromiso de mantener permanentemente actualizado el plan individual de teletrabajo.

e) Los mecanismos que garantizarán la protección y la confidencialidad de los datos objeto de tratamiento en régimen de teletrabajo.

f) El período de tiempo durante el que se desempeñarán funciones bajo esta modalidad de prestación de servicios.

g) La determinación de las jornadas teletrabajables, que podrán distribuirse de modo uniforme durante la vigencia de la autorización o no uniforme en atención a las necesidades del servicio.

El documento de compromisos podrá modificarse a instancia del teletrabajador siempre que exista acuerdo al respecto por parte del supervisor y en su caso del superior.

No obstante, los cambios de ubicación de la oficina a distancia deberán ser únicamente comunicados a la unidad de gestión competente en materia de teletrabajo, si bien exigirán declaración de que se conocen las recomendaciones de la Administración de la Comunidad de Castilla y León en materia de prevención de riesgos laborales para los teletrabajadores y compromiso de su cumplimiento en la nueva oficina a distancia.

El documento de compromisos figurará como anexo a la resolución por la que sea autorizada la prestación de servicios en régimen de teletrabajo.

9. Plan individual de teletrabajo.– Es el instrumento de seguimiento y control de la actividad del teletrabajador durante las jornadas teletrabajables.

Este documento deberá mantenerse permanentemente actualizado. Se cumplimentará tras cada jornada teletrabajable y recogerá las progresiones efectuadas por el trabajador en las funciones encomendadas. Así mismo detallará el inicio y la finalización de los períodos de interconexión.

El supervisor deberá refrendar el plan individual de teletrabajo en cada jornada presencial.

Así mismo, dicho documento podrá ser requerido en cualquier momento por la Comisión de Seguimiento del Teletrabajo.

10. Niveles de teletrabajo.– Son los tipos de teletrabajo a los que se puede acoger el solicitante de teletrabajo. Éstos son los siguientes:

a) NIVEL 1.– El empleado público desempeña sus funciones en el centro de trabajo y en la oficina a distancia.

b) NIVEL 2.– El empleado público desempeña sus funciones en el centro de trabajo, en la oficina a distancia y en aquellos lugares en los que se requiera su presencia física por razón de las funciones propias de su puesto de trabajo.

c) NIVEL 3.– El empleado público desempeña sus funciones en régimen de itinerancia, en el centro de trabajo al que se le asigne y en la oficina a distancia.

11. Comisión de Seguimiento del teletrabajo.– Es el órgano colegiado de seguimiento y control de la modalidad de prestación de servicios en régimen de teletrabajo.

12. Unidades de gestión competentes en materia de teletrabajo.– Son las unidades administrativas competentes en materia de personal en el ámbito de las Secretarías Generales, las Delegaciones Territoriales y los Organismos Autónomos.

Artículo 3. Competencias.

Son órganos competentes para la autorización del teletrabajo en la Administración General los Secretarios Generales respecto del personal de los Servicios Centrales y los Delegados Territoriales en relación con el personal destinado en los Servicios Periféricos. En el ámbito de los Organismos Autónomos esta competencia será ejercida de conformidad con sus normas de atribución competencial y, en su defecto, por el órgano con rango equivalente a Secretario General.

Artículo 4. Ámbito de aplicación.

El presente decreto será de aplicación al personal funcionario y laboral que preste servicios en la Administración General de la Comunidad de Castilla y León o en los Organismos Autónomos dependientes de ésta, que ocupe un puesto de trabajo susceptible de ser desempeñado en la modalidad de teletrabajo.

Queda fuera de su ámbito de aplicación el personal que preste servicios en centros e instituciones sanitarias de la Gerencia Regional de Salud y el personal docente que preste servicios en centros educativos.

Artículo 5. Requisitos para ser autorizado a teletrabajar.

1. La autorización de teletrabajo exigirá la concurrencia de los siguientes requisitos:

a. Subjetivos:

a.1. Estar en la situación administrativa de servicio activo. No obstante, podrá presentarse la solicitud de autorización de teletrabajo desde cualquier situación administrativa que comporte reserva del puesto de trabajo. De autorizarse dicha modalidad de prestación de servicios, habrá de solicitarse el reingreso al servicio activo.

a.2. Haber desempeñado efectivamente el puesto de trabajo que se pretende desarrollar en régimen de teletrabajo u otro de contenido similar en la misma unidad administrativa durante un período mínimo de un año dentro de los últimos dos años.

a.3. Tener los conocimientos informáticos y telemáticos teóricos y prácticos que garanticen la aptitud para teletrabajar así como la protección de los datos objeto de tratamiento.

a.4. Declarar que se conocen las medidas que propone la Administración de la Comunidad de Castilla y León en materia de prevención de riesgos laborales para los teletrabajadores y comprometerse a cumplirlas en la oficina a distancia a fecha de la autorización de teletrabajo.

a.5. Disponer en la fecha en que comience el régimen de teletrabajo del equipo informático, de los sistemas de comunicación y de la conectividad con las características que defina la Administración, en función de la disponibilidad tecnológica y la seguridad de los sistemas.

b. Objetivo: Desempeñar o tener reservado un puesto de trabajo susceptible de ser desempeñado en régimen de teletrabajo.

Son puestos susceptibles de ser desempeñados en régimen de teletrabajo los que puedan ser ejercidos de forma autónoma y no presencial atendiendo a sus características específicas y los medios requeridos para su desarrollo.

Se considerarán susceptibles de ser ejercidos en esta modalidad los puestos de trabajo cuyas funciones se puedan ejercer de forma telemática y, con carácter orientativo, aquellos puestos cuyas funciones consistan esencialmente en la elaboración de informes o estudios, la redacción de normativa, la asesoría, la corrección y la traducción de documentos.

Por sus características, no son susceptibles de ser desempeñados en régimen de teletrabajo los puestos cuyas funciones conlleven necesariamente la prestación de servicios presenciales. Se entiende por servicios presenciales aquellos cuya prestación efectiva solamente queda plenamente garantizada con la presencia física del trabajador.

Con carácter orientativo no son puestos susceptibles de ser ejercidos en régimen de teletrabajo los de las oficinas de registro y atención e información al ciudadano, los que tengan funciones de dirección, coordinación o supervisión y las secretarías de los órganos superiores y directivos.

2. El cumplimiento de los requisitos establecidos en este artículo deberá mantenerse durante el período de vigencia de la autorización de prestación de servicios en régimen de teletrabajo. Aquellos que así lo requiriesen estarán sujetos a la correspondiente comprobación por la Administración.

CAPÍTULO II

La autorización de teletrabajo

Artículo 6. La autorización de prestación de servicios en régimen de teletrabajo.

1. La autorización de la prestación de servicios en régimen de teletrabajo se realizará para el puesto que esté desempeñando el solicitante y estará condicionada en todo caso por las necesidades del servicio.

2. Cuando haya dos o más personas en una unidad administrativa o en un órgano administrativo que soliciten autorización para teletrabajar y por necesidades del servicio no sea viable concedérsela a todas, agotadas las posibilidades de rotación o de turnicidad voluntarias o de acuerdo entre los solicitantes y la Administración, la unidad de gestión competente en materia de teletrabajo aplicará el siguiente baremo para el desempate, previa comprobación de su acreditación:

a) Por conciliación de la vida familiar con la laboral.

1.º Por tener cónyuge, pareja inscrita en el registro de parejas de hecho de Castilla y León o hijos a cargo menores de edad o mayores con la patria potestad prorrogada, que tengan reconocido un grado III de dependencia: tendrán prioridad en todo caso sobre el resto de los solicitantes. En caso de haber más de un solicitante en la misma unidad administrativa en esta situación y no pudiendo autorizarse a todos ellos la prestación de servicios en régimen de teletrabajo, se establecerá un sistema de rotación obligatoria entre ellos con periodicidad semestral.

2.º Por tener cónyuge, pareja inscrita en el registro de parejas de hecho de Castilla y León o hijos a cargo menores de edad o mayores con la patria potestad prorrogada, que tengan reconocido un grado II de dependencia: 8 puntos por cada uno.

3.º Por tener cónyuge, pareja inscrita en el registro de parejas de hecho de Castilla y León o hijos a cargo menores de edad o mayores con la patria potestad prorrogada, que tengan reconocido un grado I de dependencia: 6 puntos por cada uno.

4.º Por tener hijos a cargo de las siguientes edades, de acuerdo con la escala que se especifica: De hasta 1 año, 4 puntos por cada uno; mayores de 1 año hasta 3 años, 3,5 puntos por cada uno; mayores de 3 años hasta 6 años, 3 puntos por cada uno; mayores de 6 años hasta 12 años, 1 punto por cada uno.

La percepción de puntos por los apartados 1.º, 2.º y 3.º es incompatible con la percepción de puntos por este apartado cuando se trate del mismo sujeto causante.

5.º Por ser familia monoparental con hijos a cargo de las siguientes edades, de acuerdo con la escala que se especifica: De hasta 12 años, 2 puntos por cada uno; mayores de 12 años hasta 18 años, 1 punto por cada uno.

6.º Por tener uno o varios familiares con grado II o III de dependencia, de los que se sea cuidador a efectos de la prestación económica de cuidados en el entorno familiar, siempre y cuando no estuviesen incluidos en los supuestos anteriores: 5 puntos por cada uno.

7.º Por tener uno o varios familiares con grado II o III de dependencia, que sean usuarios del servicio de ayuda a domicilio y de los que se sea cuidador familiar en exclusiva, según certificado expedido por la Gerencia Territorial de Servicios Sociales correspondiente a su domicilio, siempre y cuando no estuviesen incluidos en los supuestos anteriores: 4 puntos por cada uno.

8.º Por tener uno o varios familiares hasta el segundo grado que padezcan una enfermedad muy grave o grave en situación aguda: 4 puntos por cada uno. La gravedad de la enfermedad se acreditará mediante certificado médico.

Las referencias realizadas a hijos se entienden hechas a los naturales y adoptivos, así como a aquellas personas que se encuentren en régimen de tutela o acogimiento, tanto del empleado público como de su cónyuge o pareja de hecho.

Las referencias realizadas a familiares incluyen el parentesco por consanguinidad y afinidad y dentro de este último, la relación entre el empleado público y los parientes por consanguinidad de su cónyuge o pareja de hecho.

El baremo establecido en los apartados anteriores sólo será de aplicación en aquellos supuestos en que el cónyuge o la pareja de hecho desempeñe una actividad por cuenta propia o ajena o cuando no desempeñándolas se encuentre incapacitado para dicho cuidado por razones de salud debidamente acreditadas. Así mismo, el baremo no será aplicado cuando el cónyuge o la pareja de hecho presten servicios en la modalidad de teletrabajo en la Administración de la Comunidad de Castilla y León.

b) Por causas de salud: Por tener el empleado público reconocido un grado de dependencia, una discapacidad con movilidad reducida o tener una enfermedad que curse por brotes que impidan el normal desenvolvimiento en la realización de las actividades de la vida diaria, se aplicará la siguiente escala:

1.º Si la discapacidad es superior al 45% o el grado de dependencia es superior a I: 5 puntos.

2.º Si la discapacidad está comprendida entre el 33% y el 45% y el grado de dependencia es I: 3 puntos.

3.º Si se trata de enfermedad que cursa por brotes que impidan el normal desenvolvimiento: 4 puntos.

c) Por desplazamiento: Por existir una distancia superior a 30 kilómetros entre el domicilio y el centro de trabajo del empleado público, 1 punto.

d) Por formar parte de un colectivo de especial protección, con excepción de los afectados por causa de discapacidad, siempre y cuando el solicitante de teletrabajo justifique que esta modalidad de prestación de servicios, como consecuencia de sus circunstancias especiales, contribuye a mejorar sus circunstancias personales, familiares o laborales: 3 puntos.

e) Por la realización de estudios: Por realizar estudios reglados presenciales, 1 punto.

f) Por no desempeñar otro puesto de trabajo, cargo o actividad compatible en el sector público o privado: 0,5 puntos.

3. En caso de igualdad en la puntuación total, se usará como criterio de desempate la puntuación más alta obtenida en los diferentes apartados en el orden en que están indicados.

De persistir el empate, se autorizará a quien en igualdad de condiciones no haya tenido concedida durante los veinticuatro meses consecutivos inmediatamente anteriores la prestación de servicios mediante la modalidad de teletrabajo.

En última instancia se elegirá por sorteo público a la persona que ha de disfrutar de la prestación de servicios en régimen de teletrabajo.

4. La desaparición de las circunstancias objeto de baremación que hayan sido tenidas en cuenta para autorizar el teletrabajo, habrá de comunicarse a la unidad de gestión competente en materia de teletrabajo en el plazo máximo de tres días.

Artículo 7. Duración y prórroga de la autorización de teletrabajo.

1. La autorización de teletrabajo tendrá una duración máxima de un año, sin perjuicio de las posibilidades de suspensión, pérdida de efectos, renuncia o extinción automática.

2. No obstante, quince días antes de que llegue a término el plazo por el que se concedió el teletrabajo, el empleado público podrá solicitar la prórroga de la autorización al órgano competente para su concesión, que podrá concederla o denegarla mediante resolución, previo informe del superior.

El otorgamiento de la prórroga se encontrará condicionado al mantenimiento de los requisitos y de las necesidades del servicio que dieron lugar a la autorización inicial, así como a la inexistencia de otros solicitantes de teletrabajo en la unidad administrativa u órgano administrativo en el que el teletrabajador preste servicios.

La duración de cada prórroga será como máximo de un año y podrán solicitarse tantas prórrogas como se desee, siempre y cuando se cumplan las condiciones enunciadas.

Artículo 8. Suspensión de la autorización de teletrabajo.

1. Cuando existan circunstancias sobrevenidas que afecten al teletrabajador o cuando las necesidades del servicio lo justifiquen, se podrá suspender la autorización de teletrabajo a instancia del teletrabajador o del superior, previo informe del supervisor.

Son circunstancias sobrevenidas aquellas que no pudieron ser tenidas en cuenta en el momento de autorizarse el teletrabajo pero que no se encuentran incluidas dentro de las causas de pérdida de efectos de la autorización de teletrabajo previstas en el artículo 9.

2. El período de tiempo durante el que la autorización de teletrabajo se encuentre suspendida no será computable a efectos del período máximo para el que éste hubiese sido autorizado.

3. La resolución de suspensión de teletrabajo será dictada por el órgano competente para su autorización.

Artículo 9. Pérdida de efectos de la autorización de teletrabajo.

1. La resolución de autorización de teletrabajo quedará sin efecto cuando concurra alguna de las causas siguientes:

a) Necesidades del servicio debidamente motivadas.

b) Incumplimiento sobrevenido del requisito de disponer de un equipo informático y de los sistemas de comunicación y seguridad adecuados para teletrabajar, así como de disponer de una conexión efectiva.

c) Modificación sustancial de las funciones o tareas desempeñadas por el empleado público.

d) Incumplimiento del contenido del documento de compromisos o en relación con la actualización del plan individual de teletrabajo.

e) Deficiencias en la prestación del servicio.

f) Concurrencia de causas sobrevenidas graves cuya duración resulte impredecible, que afecten a la prestación del servicio.

g) Incumplimiento del deber de comunicar o no comunicar en plazo, la desaparición de las causas objeto de baremación cuando éstas se hubiesen tenido en cuenta para autorizar el teletrabajo. Si el teletrabajador no renuncia a la autorización pero existen más solicitudes de teletrabajo en la unidad administrativa que no pueden concederse simultáneamente, agotadas las posibilidades de rotación y turnicidad se procederá a la rebaremación de todos ellos, actuándose en caso de empate de acuerdo con lo dispuesto en el artículo 6.3.

h) Desaparición de las circunstancias objeto de baremación que dieron lugar a la autorización, cuando existan otros miembros de la unidad o el órgano administrativo cuya autorización no resulte compatible con la anterior, que obtengan mejor puntuación una vez aplicado dicho baremo.

2. La pérdida de efectos de la autorización de teletrabajo será declarada de oficio por resolución motivada del órgano competente para la autorización, a propuesta del supervisor, una vez emitido el informe correspondiente por el superior y previa audiencia del teletrabajador.

Artículo 10. Renuncia a la prestación de servicios en régimen de teletrabajo.

El teletrabajador podrá renunciar sin alegar causa alguna a la autorización de teletrabajo antes de que ésta llegue a término, con un preaviso mínimo de quince días. El órgano competente para acordar dicha autorización deberá dictar resolución declarativa de esta circunstancia.

Artículo 11. Extinción automática del teletrabajo.

La autorización de la prestación de servicios en régimen de teletrabajo finalizará automáticamente, por las siguientes causas:

a) Por llegar a término el tiempo por el que se otorgó o en su caso por el que se prorrogó.

b) Por cambiar el empleado público de puesto de trabajo.

c) Por dejar de estar en la situación administrativa de servicio activo, aun cuando con posterioridad se vuelva a ocupar el mismo puesto de trabajo que dio lugar en su día a la autorización de teletrabajo.

d) Por mutuo acuerdo entre las partes.

Artículo 12. Reincorporación a la prestación de servicios en régimen presencial.

La pérdida de efectos, la renuncia o la extinción de la autorización conllevarán la reincorporación a la prestación de servicios en régimen presencial.

Artículo 13. Denegación de la autorización de teletrabajo.

La solicitud de teletrabajo será denegada cuando concurra alguna de las siguientes causas:

a) No reunir los requisitos para teletrabajar recogidos en el artículo 5.

b) Cambiar de puesto de trabajo con posterioridad a la solicitud y antes de la autorización.

c) Necesidades del servicio de acuerdo con lo previsto en el artículo 6.1.

d) No obtener u obtener peor puntuación una vez aplicado el baremo al que se refiere el artículo 6.2, cuando en la unidad administrativa existiesen varias solicitudes de teletrabajo no susceptibles de ser autorizadas simultáneamente.

e) No remitir el documento de compromisos debidamente cumplimentado y firmado o no hacer efectiva la conexión informática en el plazo otorgado en el artículo 23.1.a) 2.ª, por causa imputable al solicitante de teletrabajo.

CAPÍTULO III

Régimen jurídico del teletrabajador

Artículo 14. Igualdad de derechos y deberes.

Salvo las especificidades contenidas en esta norma, el teletrabajador tendrá los mismos derechos y deberes que el resto del personal de la Administración General de la Comunidad de Castilla y León y de los Organismos Autónomos dependientes de ésta.

Artículo 15. Especialidades en materia de jornada.

1. La jornada de trabajo de los teletrabajadores se distribuirá de forma que éste preste servicios al menos un día de la semana de forma presencial.

2. La parte presencial de la jornada será proporcionalmente la misma, en cómputo mensual, a la correspondiente al desempeño del puesto sin régimen de teletrabajo.

3. En cuanto a la parte no presencial de la jornada, el teletrabajador habrá de acreditar a través del plan individual de teletrabajo tanto el cumplimiento de las obligaciones recogidas en el documento de compromisos como de las establecidas durante las jornadas presenciales. Así mismo, habrá de acreditar la satisfacción de los períodos de interconexión.

Los períodos de interconexión comprenderán necesariamente la parte no flexible de la jornada ordinaria, que en todo caso podrá someterse a las adaptaciones de horario previstas en la normativa vigente por razones de conciliación de la vida familiar y laboral.

4. Los teletrabajadores que tengan concedida una reducción de jornada tendrán que aplicar proporcionalmente dicha reducción a la jornada presencial y a la jornada teletrabajable.

5. En ningún caso la jornada diaria podrá fraccionarse para su prestación en ambas modalidades.

6. Podrá exigirse la presencia del teletrabajador en el centro de trabajo durante jornadas teletrabajables cuando ésta sea necesaria por razones del servicio. Deberá dejarse constancia de tales circunstancias en el plan individual de teletrabajo. Siempre que sea posible, se le convocará a tal efecto con una antelación mínima de cuarenta y ocho horas.

Artículo 16. Especialidades en materia de permisos.

Los permisos susceptibles de disfrute en las jornadas teletrabajables deberán ser solicitados y justificados en los términos establecidos reglamentariamente con carácter general.

Artículo 17. Especialidades en materia de incompatibilidades.

A efectos del régimen de incompatibilidades del personal al servicio de la Administración de la Comunidad de Castilla y León, se tomará en consideración la jornada y el horario de trabajo correspondiente al puesto de trabajo desempeñado por el teletrabajador en los mismos términos que si éste no fuese desempeñado en régimen de teletrabajo.

Artículo 18. Especialidades en materia de formación.

Tanto el teletrabajador como el supervisor, recibirán formación en materia de prestación de servicios en régimen de teletrabajo.

El teletrabajador tendrá obligación de recibir la formación a la que fuese convocado a tal efecto, salvo que razones del servicio debidamente motivadas lo impidiesen.

Artículo 19. Especialidades en materia de equipamiento.

1. El equipamiento básico para la prestación de servicios durante las jornadas teletrabajables, será aportado por los empleados públicos y estará constituido por un ordenador personal dotado de los sistemas de comunicación que defina la Administración en función de la disponibilidad tecnológica y la seguridad de los sistemas, así como por un teléfono de contacto cuyo número será obligatoriamente facilitado al supervisor.

2. Corresponderá al teletrabajador solucionar las incidencias imputables a su equipo informático y a la conectividad.

3. La conexión con los sistemas informáticos de la Administración Autonómica deberá llevarse a cabo a través de los sistemas que la Administración determine para garantizar la accesibilidad, agilidad, seguridad y confidencialidad de la información.

Artículo 20. Prevención de riesgos laborales.

1. El lugar determinado como oficina a distancia por parte del teletrabajador deberá cumplir con la normativa vigente en materia de prevención de riesgos laborales, prestando especial atención a los aspectos relacionados con la seguridad y la ergonomía.

2. Una vez autorizado el teletrabajo, el servicio de prevención responsable de la evaluación del puesto remitirá al teletrabajador el correspondiente autocuestionario de prevención de riesgos laborales, que será devuelto debidamente cumplimentado y firmado para la valoración del mismo. Será responsabilidad del empleado público el cumplimiento de lo declarado en el autocuestionario así como la adopción de las medidas correctoras que se le propongan.

3. A los efectos de contingencias profesionales será de aplicación la normativa vigente en materia de accidentes de trabajo y enfermedades profesionales.

CAPÍTULO IV

Procedimiento para la autorización de teletrabajo

Artículo 21. Solicitud.

1. Los empleados públicos dirigirán sus solicitudes de teletrabajo al órgano competente para su autorización.

2. La solicitud de teletrabajo deberá contener:

a) Declaración de que se cumplen a fecha de la solicitud o de que se cumplirán a fecha de la autorización, los requisitos subjetivos a los que se refiere el artículo 5.1 en sus apartados a1, a2 y a3.

b) Jornadas que pretenden ser desempeñadas en régimen de teletrabajo.

c) La ubicación de la oficina a distancia.

d) Declaración de que se poseen a fecha de la solicitud o de que se poseerán a la fecha en la que haya de realizarse la conexión informática, los dispositivos electrónicos así como la conexión a internet adecuados para teletrabajar.

e) Declaración de que se han leído las recomendaciones en materia de prevención de riesgos laborales facilitadas por la Administración y compromiso de que a la fecha de inicio de la autorización del teletrabajo, en caso de producirse, éstas se cumplirán en la oficina a distancia.

3. La solicitud de teletrabajo se realizará electrónicamente a través de la sede electrónica de la Administración de la Comunidad de Castilla y León o de medio similar habilitado al efecto por ésta.

Artículo 22. Informe del superior.

Recibida la correspondiente solicitud, en el plazo máximo de diez días las unidades administrativas competentes en materia de personal recabarán informe preceptivo del superior, que deberá ser evacuado también en el plazo máximo de diez días y que habrá de pronunciarse como mínimo sobre:

a) Si el solicitante tiene los conocimientos informáticos y telemáticos teóricos y prácticos que garanticen la aptitud para teletrabajar así como sobre la protección de los datos objeto de tratamiento.

b) Si el puesto de trabajo cumple los requisitos para poder ser desempeñado en régimen de teletrabajo.

c) Si las necesidades del servicio son compatibles con la autorización de teletrabajo.

En dicho informe propondrá la concesión o la denegación de la autorización de teletrabajo. Las propuestas denegatorias deberán ser debidamente motivadas y si estriban en necesidades del servicio éstas habrán de ser especificadas.

En caso de ser favorable a la concesión, propondrá la designación del supervisor, que podrá ser él mismo o un tercero.

Artículo 23. Resolución.

1. Emitido el informe citado en el apartado anterior, el órgano competente para la autorización del teletrabajo:

a) En caso de considerar estimable la solicitud, procederá a la realización de las siguientes actuaciones:

1.ª Comunicará al empleado público correspondiente su designación como supervisor en caso de no ser éste la misma persona que el superior.

2.ª Pondrá en conocimiento del solicitante que su solicitud es estimable de acuerdo con el informe del superior y le comunicará quién será su supervisor en caso de autorizarse el teletrabajo. Así mismo, le otorgará un plazo de diez días para que proceda al cumplimiento de los siguientes requisitos:

i. La remisión del documento de compromisos firmado por él, por el supervisor y en su caso por el superior a la unidad de gestión competente en materia de teletrabajo.

ii. La efectividad de la conexión informática necesaria para la prestación de servicios en dicho régimen en condiciones de eficiencia y seguridad por la unidad de informática competente.

3.ª En caso de acreditarse el cumplimiento de los requisitos citados, dictará resolución por la que:

i. Autorizará el teletrabajo en los términos establecidos en el documento de compromisos.

ii. Indicará la fecha de inicio y finalización de la autorización de teletrabajo.

iii. Especificará la puntuación total obtenida en aplicación del baremo recogido en el artículo 6, en caso de haber resultado determinante para conceder la autorización.

iv. Comunicará que la autorización de teletrabajo finalizará automáticamente de concurrir alguna de las causas a las que se refiere el artículo 11.

b) Podrá dictar resolución denegatoria de la autorización de prestación de servicios en régimen de teletrabajo, motivada en alguna de las causas previstas en el artículo 13.

2. Cuando el órgano competente para resolver sea el Delegado Territorial, deberá solicitar informe preceptivo al correspondiente Secretario General con carácter previo a la denegación de la autorización de teletrabajo, así como al dictado de la comunicación a la que se refiere el apartado 1.a) 2.ª de este artículo.

3. Tanto la comunicación del apartado 1.a) 2.ª, como las resoluciones de autorización y denegación de prestación de servicios en régimen de teletrabajo, serán notificadas electrónicamente por el procedimiento de comparecencia en la sede electrónica de la Administración de la Comunidad de Castilla y León o bien por el procedimiento que establezca la normativa vigente en materia de administración electrónica y que sea habilitado a tal efecto en esta Administración.

4. Deberá remitirse copia de todas las resoluciones denegatorias a la Comisión de Seguimiento del Teletrabajo.

Artículo 24. Plazo máximo para resolver.

Las solicitudes de teletrabajo deberán resolverse y notificarse en el plazo máximo de tres meses. La falta de pronunciamiento expreso por parte de la Administración en el plazo mencionado tendrá efectos desestimatorios.

CAPÍTULO V

Comisión de seguimiento del teletrabajo

Artículo 25. Concepto y composición.

1. Es el órgano colegiado de seguimiento y control de la modalidad de prestación de servicios en régimen de teletrabajo. Se encuentra adscrito al titular de la Dirección General con competencias en materia de Función Pública y está constituido por los siguientes miembros:

a) Presidente: Será quien ostente la titularidad de la Dirección General de la Función Pública o la persona en quien delegue. Será suplido en caso de ausencia por el vocal al que designe expresamente.

b) Cinco vocales: Serán elegidos por quien ostente la presidencia. Tres desempeñarán puestos de trabajo con funciones de gestión de personal funcionario, gestión de personal laboral y prevención de riesgos laborales respectivamente, en la Dirección de la Función Pública. Uno prestará servicios en materia de personal en el ámbito de una Delegación Territorial y otro en el de una Secretaría General.

c) Secretario: Será designado por quien ostente la presidencia de entre los vocales.

2. La constitución de la Comisión de Seguimiento del Teletrabajo se realizará por resolución del titular de la Dirección General de la Función Pública, que será publicada en el Boletín Oficial de Castilla y León.

Artículo 26. Competencias.

Son competencias de la Comisión de Seguimiento del Teletrabajo las siguientes:

a) Estudiar las incidencias que le hagan llegar las unidades de gestión competentes en materia de teletrabajo y dictar instrucciones para su resolución.

b) Establecer criterios orientativos en relación con los puestos excluidos del régimen de teletrabajo. Dichos criterios serán publicados en la sede electrónica de la Junta de Castilla y León.

c) Elaborar y valorar cuestionarios destinados a evaluar el funcionamiento de la prestación de servicios en régimen de teletrabajo, así como el índice de satisfacción de los teletrabajadores, los supervisores y el resto de la organización.

d) Informar las quejas que se presenten en relación con la prestación de servicios en régimen de teletrabajo.

e) Elaborar un informe anual con las conclusiones obtenidas de los apartados c) y d).

f) Controlar los expedientes de teletrabajo tramitados. A tal efecto, realizarán un muestreo que alcanzará como mínimo al 25% de los expedientes de teletrabajo autorizados anualmente, en relación con la existencia y la permanente actualización que debe mantener el plan individual de teletrabajo.

g) Recabar y mantener actualizada la legislación vigente en materia de teletrabajo tanto en ésta como en otras Administraciones Públicas, así como sus experiencias al respecto.

Artículo 27. Periodicidad de las reuniones.

Las reuniones de la comisión de seguimiento del teletrabajo se realizarán con una periodicidad mínima trimestral.

DISPOSICIÓN TRANSITORIA

Régimen de las autorizaciones existentes

1. Las autorizaciones de prestación de servicios en régimen de teletrabajo existentes a la entrada en vigor del presente decreto, se mantendrán vigentes durante 6 meses

contados desde el día siguiente al de dicha entrada en vigor. No obstante, su validez estará condicionada a la formalización del correspondiente documento de compromisos en el plazo máximo de un mes contado desde la mencionada entrada en vigor, así como al cumplimiento de las obligaciones relacionadas con el plan individual de teletrabajo. A tal efecto, figurará como supervisor quien viniese desempeñando las funciones de organización del trabajo y de seguimiento del teletrabajador.

La falta de formalización del documento de compromisos en el plazo señalado, el incumplimiento de las obligaciones derivadas del plan individual de teletrabajo o la suma de ambas circunstancias, conllevará la extinción de la autorización.

2. Las prórrogas de las autorizaciones previas a la entrada en vigor del presente decreto, se regirán por las normas establecidas en él.

DISPOSICIÓN DEROGATORIA

Derogación normativa

La presente disposición deroga el Decreto 9/2011, de 17 de marzo, por el que se regula la jornada de trabajo no presencial mediante teletrabajo en la Administración de la Comunidad de Castilla y León.

DISPOSICIONES FINALES

Primera.– Habilitación.

Se faculta al titular de la consejería competente en materia de función pública para dictar Órdenes en aplicación de este decreto.

Segunda.– Entrada en vigor.

El presente decreto entrará en vigor el día siguiente al de su publicación en el Boletín Oficial de Castilla y León.

Valladolid, 7 de junio de 2018.

El Presidente de la Junta
de Castilla y León,
Fdo.: Juan Vicente Herrera Campo

El Consejero de la Presidencia,
Fdo.: José Antonio de Santiago-Juárez López

CV: BOCYL-D-13062018-1