



Medidas y recomendaciones en materia de telecomunicaciones durante el estado de alerta por el COVID-19

Las compañías operadoras de telecomunicaciones adquieren los siguientes compromisos

- ✓ Las operadoras no podrán suspender ni interrumpir los servicios que sus clientes tuviesen contratados en el momento de la declaración del estado de alarma.
- ✓ Se han suspendido todas las operaciones de portabilidad de numeración fija y móvil en las que sea necesaria la visita de un técnico para poder realizarla.
- ✓ Las operadoras reforzaran todos los trabajos técnicos que sean necesarios, haciendo los mayores esfuerzos para garantizar la conectividad, las capacidades de operación y la agilidad de respuesta ante incidentes.
- ✓ Los radiodifusores deben mantener la operativa necesaria para garantizar la adecuada prestación del servicio de radiodifusión de la televisión digital terrestre digital.

Se recomienda a la ciudadanía hacer un uso responsable de los servicios de telecomunicaciones para garantizar el buen funcionamiento de la red

- ✓ Descargar solo los documentos o archivos que sean realmente necesarios, y si pueden esperar, hacerlo por la noche o en las horas con menos concurrencia de tráfico, entre las 14:00 y las 16:00 horas y entre las 00:00 y las 08:00 horas.
- ✓ Siempre que sea posible, **no enviar ficheros de mucho peso**, sino enlaces o rutas hacia donde estén almacenados. Y, si es imprescindible enviarlos, **comprimirlo antes o darles un formato que pese menos**.
- ✓ Usar el teléfono fijo en vez del móvil para realizar llamadas cuando sea posible. E incluso hacer llamadas a través del teléfono fijo en vez de usar mensajería o video llamadas.
- ✓ Reservar para las horas de menos tráfico el uso de herramientas de ocio, videojuegos, streaming, o reproducción de vídeos en directo.



Consejos de seguridad en el uso intensivo de internet durante el Estado de Alerta por el Covid-19

- ✓ **No facilitar datos personales si no existe una completa seguridad sobre quién los va a recibir.**
- ✓ **Exija, siempre, "conexiones seguras".** Asegúrese que, al transmitir datos sensibles, la dirección de internet empieza por **https** y va **acompañada de un candado cerrado o una llave**. Compruebe los certificados de seguridad, en páginas que requieren datos personales.
- ✓ **Utilice un buen producto antivirus y actualizarlo, frecuentemente.** Estos antivirus pueden contener distintas operatividades como por ejemplo funciones anti-phishing que analizan las páginas de acceso para verificar que son seguras y no se roba la identidad. Además de antivirus hay que protegerse con programas anti-spyware, malware y hardware.
- ✓ **Extreme la precaución a la hora de abrir archivos que reciben por e-mail, de páginas web no seguras, en sesiones de chat o cualquier otro medio.**
- ✓ **Actualice los sistemas operativos y navegadores,** con los parches que publican las firmas especializadas de software.



<https://www.boe.es/buscar/act.php?id=BOE-A-2020-3824>



https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4208