Ciberseguridad básica en el teletrabajo

En la Organización

Proveer VPNs para la conexión de todos los usuarios, a ser posible con doble factor de autenticación y/o restricción por MAC de tipo whitelist.

Emplear contraseñas complejas, preferiblemente de 24 caracteres o más, incluyendo letras mayúsculas, minúsculas, números y caracteres especiales. Gestionándolas con gestores de contraseñas.

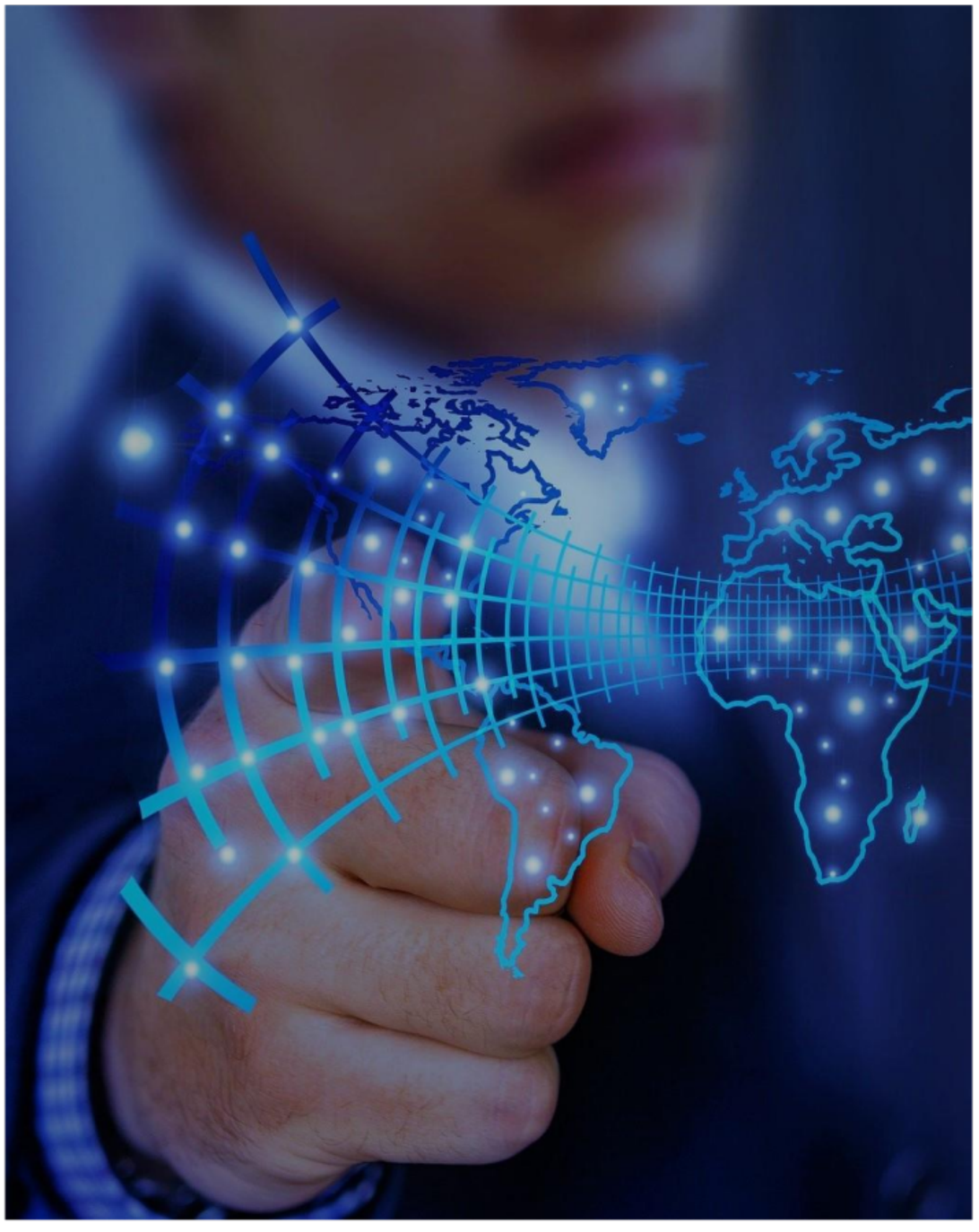
Cumplir el principio de mínima exposición posible en todos los equipos y servidores. Es decir, comprobar que puertos se tienen abiertos y cuáles de éstos son realmente necesarios e imprescindibles para desempeñar la labor.

Restricción de permisos de usuario en los equipos y en el acceso a los datos corporativos.

Establecer canales internos de comunicación y plataformas seguras.

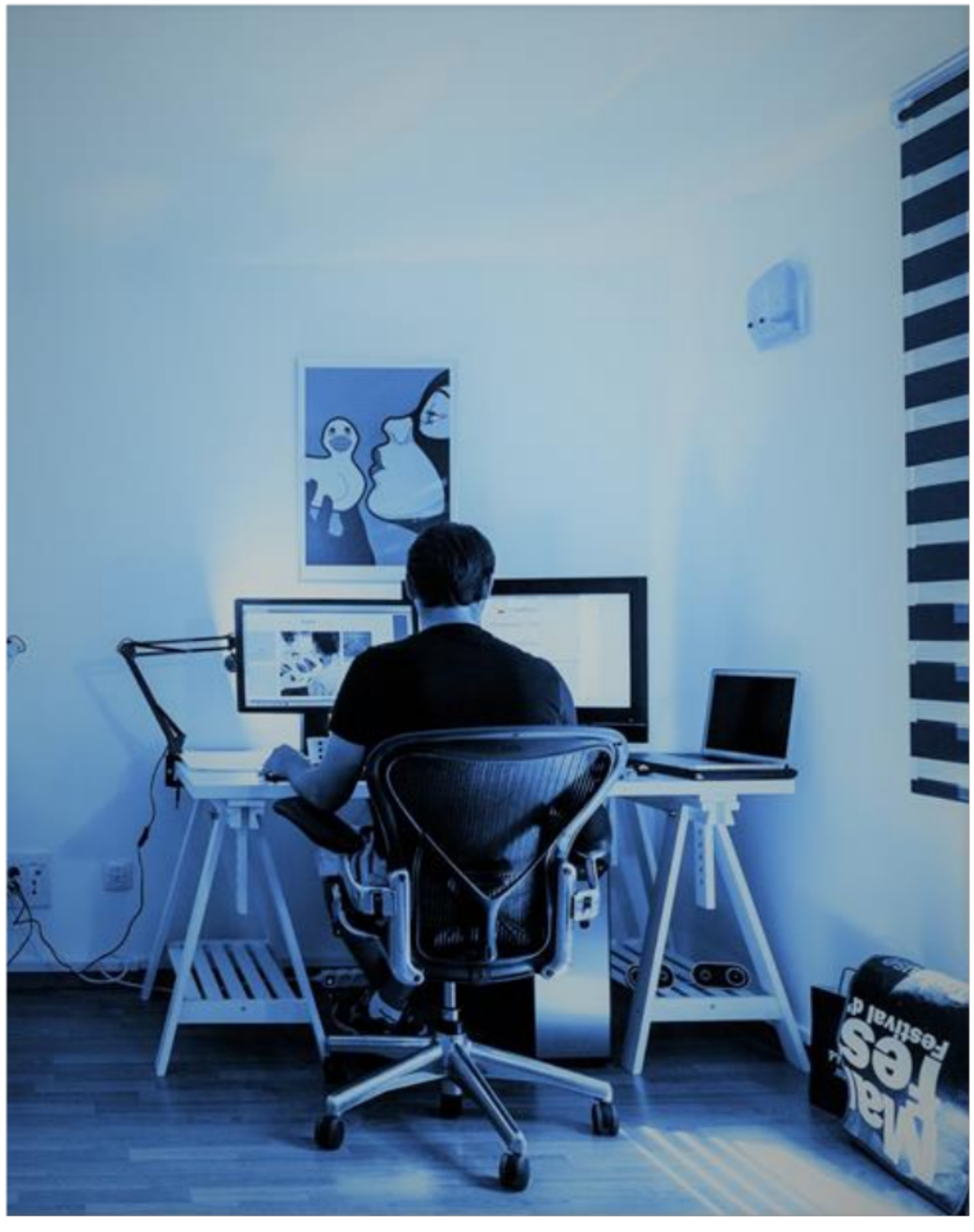
Mantener sistema operativo, aplicaciones y antivirus actualizados, con el fin de minimizar las vulnerabilidades.

Uso de DNS con protección y que ofrezcan logs.



Ciberseguridad básica en el teletrabajo

En el domicilio



Si es posible utilizar los equipos y sistemas de comunicación que la propia empresa nos ha facilitado.

Renovar de forma habitual las contraseñas del Wi-Fi y del router y no compartirlas con nadie.

Acceder solo a sitios web seguros y estar muy atento a los correos que remiten personas conocidas con asuntos o expresiones no habituales.

Emplear VPN para la conexión con la red de la empresa.

Al terminar una videoconferencia, ocultar la cámara.

Seguir las políticas de seguridad establecidas por la empresa.