A continuación se incluye un listado de medidas de seguridad recomendadas que el empleado debe aplicar cuando se encuentre fuera de las instalaciones. Se recomienda proporcionar esta información a los empleados cuando se les entregue un portátil o cualquier otro dispositivo portátil.

MEDIDAS DE SEGURIDAD BÁSICAS

Verificar si la política de seguridad de nuestra empresa permite conectar a redes ajenas y las condiciones para ello.

Cuando exista la posibilidad de conectar por cable, desconectar las redes Wi-Fi y Bluetooth si no se van a utilizar.

Mantener el equipo permanentemente actualizado.

Mantener el antivirus permanentemente actualizado y en funcionamiento.

Al conectar a una nueva red inalámbrica, comprobar que la red a la que se va a conectar es segura: protocolo WPA o preferiblemente WPA2.

En el caso de conectar a redes públicas, siempre establecer la configuración de la red a “Pública”. Nunca seleccionar “casa” o “trabajo”.

En la conexión remota a la red de la empresa, establecer conexión VPN para proteger las comunicaciones.

Al navegar por Internet, verificar que las direcciones de destino son correctas y que el certificado es válido, cuando se trate de conexiones a entornos seguros (webmail, extranet, etc.)

Al recibir correos electrónicos, desconfiar de aquellos que lleven adjuntos sospechosos, provengan de desconocidos o no hayan sido solicitados.

Al intercambiar ficheros por mensajería instantánea, almacenamiento en la nube, etc., cifrar los ficheros antes del envío.

MEDIDAS DE SEGURIDAD AVANZADAS

Si es posible, configurar los servidores DNS de confianza en lugar de los que la propia red asigne automáticamente.

Desactivar las opciones de IPv6 si no se van a utilizar.

Desactivar en el equipo aquellos servicios innecesarios como Wpad, Wins, Netbios, o similares.