madriddigital
Agencia para la Administración Digital de la Comunidad de Madrid

Comunidad de Madrid
CONSEJERÍA DE PRESIDENCIA

RECOMENDACIONES DE SEGURIDAD DE LA INFORMACIÓN PARA EL TRABAJO REMOTO DE LA COMUNIDAD DE MADRID.

AGENCIA PARA LA ADMINISTRACIÓN DIGITAL DE LA COMUNIDAD DE MADRID

OFICINA DE GOBIERNO DE SEGURIDAD

Contenido

1 INTRODUCCIÓN

RECOMENDACIONES DE SEGURIDAD DE LA INFORMACIÓN PARA EL TRABAJO REMOTO DE LA COMUNIDAD DE MADRID.

Ante la situación excepcional que estamos viviendo por el COVID-19 (Coronavirus), desde la Madrid Digital, la Oficina de Gobierno de Seguridad os facilitamos unas recomendaciones de seguridad básicas para el trabajo remoto, tanto para aquellos empleados que dispongáis de equipo corporativo como para aquellos que hagáis uso de vuestro equipo personal.

El trabajo remoto es una de las maneras más efectivas de luchar contra el coronavirus, permitiendo mantener la actividad productiva y el servicio. Pero el trabajo remoto cambia modos, hábitos y espacios, por lo que hay que tomar **recomendaciones para que la información de los ciudadanos y los servicios de la Comunidad de Madrid se mantenga segura**

2 USUARIO

Login y contraseñas

- Establece un login y contraseña específicos para el acceso a tu equipo particular para trabajo remoto.
  - Establece un usuario de acceso al equipo protegido por contraseña diferenciado para hacer trabajo remoto desde tus equipos particulares.
- Establece contraseñas robustas y solo conocidas por ti:
  - No utilices las contraseñas por defecto o utilizadas con anterioridad.
  - No compartas las contraseñas con nadie.
  - Deben ser difíciles de adivinar o calcular, no utilices elementos o palabras que puedan ser públicas o fácilmente adivinables (ej. nombre + fecha de nacimiento).
  - Utilizar la concatenación de varias palabras para construir contraseñas largas (passphrases) debe procurar que la deducción, automática o no, no sea simple. Por ejemplo: “elefanteneumáticocarpeta”.
  - No utilices la misma contraseña para uso profesional y doméstico.
  - Cambia las contraseñas periódicamente.
- Desactiva o rechaza en el navegador web las opciones de recordar o guardar las contraseñas.
- En tus pausas o descansos bloquea siempre la sesión de equipo.
  - Bloquea siempre la sesión del equipo ante cualquier ausencia temporal, aunque sea por poco espacio de tiempo.
- Cierra todas las conexiones y sesiones abiertas en tus equipos al finalizar tu jornada.
  - Al finalizar tu jornada laboral recuerda cerrar todas las conexiones y sesiones establecidas desde tu equipo corporativo o particular.

3 EQUIPOS

- **Si utilizas ordenadores corporativos**
  - Utiliza siempre que sea posible los equipos corporativos proporcionados.
    - Utiliza equipos proporcionados por la Comunidad de Madrid, es la mejor opción y más segura. Si no es posible, podrás utilizar el ordenador personal propio, teniendo en cuenta las recomendaciones de seguridad establecidas.
  - Los equipos proporcionados por la Comunidad de Madrid son exclusivos para el trabajador y solo para fines profesionales.
    - Recuerda que el uso es exclusivo por parte del trabajador (no compartido con terceros) y solo para fines profesionales.
  - No instales software no corporativo o no autorizado en los equipos proporcionados por Comunidad de Madrid.
  - No saques de tu domicilio los equipos corporativos proporcionados, sin causa justificada.
- **Si utilizas ordenadores particulares**
  - Cuando uses equipos particulares, hazlo siempre aplicando las recomendaciones de seguridad.
  - Instala y actualiza regularmente las actualizaciones de seguridad del sistema y un programa antivirus en el ordenador particular.
    - Es importante disponer de un programa antivirus activo en el ordenador personal, así como, asegúrate que se actualizan de manera frecuente dichos programas. En el mercado existen algunos antivirus gratuitos:

      (https://www.osi.es/es/herramientas-gratuitas?combine=&herramienta_selec%5B%5D=115).
  - No compartas tu equipo particular para trabajo remoto con terceras personas, en lo posible.
    - En la medida de lo posible, no compartas el ordenador con terceras personas, de este modo garantizaras que solo se instala software autorizado y se acceden a sita web de confianza.

4 COMUNICACIONES Y CONEXIONES REMOTAS

- **Conexiones remotas**
  - Siempre que sea posible utiliza con los sistemas de la Comunidad de Madrid conexiones de red privada virtual (VPN), o alternativamente las soluciones seguras de conectividad remota facilitadas.
    - Si dispones de una conexión de Red Privada Virtual (VPN), conéctate siempre a los sistemas corporativos a través de ella. En caso de no disponer de VPN, procura utilizar las soluciones seguras de conectividad remota proporcionados o facilitados por la Comunidad de Madrid.
  - Utiliza solo redes Wi-Fi privadas protegías por contraseña, evitando redes Wi-Fi públicas o abiertas.
  - Asegúrate de que tu red Wi-Fi doméstica dispone de contraseña y protocolos de encriptación AES.
  - Conéctate a sitios web a través de canales de comunicación segura, mediante protocolos "https" (candado).

- **Navegadores y comunicaciones con terceros**

  - Utiliza navegadores web con las actualizaciones de seguridad recomendadas por el fabricante.
  - Limita el envío de imagen, anexos y documentos en tus comunicaciones, a fin de evitar sobrecarga de la red www.
  - Revisa con tu antivirus los anexos y documentos enviados o descargados en tus comunicaciones, garantizando así que estén libres de malware.
  - Realiza transacciones o descargas de ficheros solo desde sitios web de confianza, evitarás malware, virus o secuestro de datos.

5 ACCESO Y COPIAS DE SEGURIDAD

- **Acceso a la información y almacenamiento**

  - No descargues información de los sistemas de la C. de Madrid en los equipos de trabajo, hazlo solo si es imprescindible.
  - Si necesitas descargar datos, almacena la información de trabajo sólo en Onedrive, evita usar discos duros externos, cds, usb, etc...
    - Con carácter general la información que sea imprescindible extraer de los sistemas para el mejor desarrollo del trabajo remoto, se debe almacenar en Onedrive.
  - Trata la información personal mínima y necesaria, y siempre en relación con los fines para la que ha sido recogida.
  - Pide autorización a tu responsable para descargar información con datos personales.
  - Protege la información sensible o personal en tu equipo mediante contraseña de acceso o cifrado.
    - No copies información sensible en tus dispositivos o dispositivos extraíbles. En caso imprescindible, es necesario aplicar claves de acceso o algoritmos de cifrado.
  - Elimina toda la información almacenada en equipos o dispositivos una vez que deje de ser necesaria.

6 PHISING, SOFTWARE Y MALICIOSO Y FAKE NEWS

- Desconfía de peticiones de claves, datos personales o contraseñas, aun cuando parezca de origen conocido.
- Descarga apps móviles exclusivamente desde tiendas oficiales (google store o apple store), evitarás malware, virus o secuestro de datos.
  - Existen numerosas campañas de intrusión en dispositivos a través de apps maliciosas aparentemente inofensivas pero que pueden ser la puerta de entrada de malware a tus equipos y de ahí a la información y los sistemas de la Comunidad de Madrid.
- Evita abrir correos, enlaces web o anexos de origen desconocido o sospechoso, evitarás malware, virus o secuestro de datos.
  - Evita abrir correos de origen desconocido o sospechoso. Existen numerosas campañas de ataques de phising y malware usando correos que suplantan la identidad de terceros o que envían información falsa (por ej: "¿cómo protegerte del coronavirus?" "cura del coronavirus").

7 COMUNICACIÓN DE INCIDENCIAS

- Comunica, lo antes posible, a tu responsable cualquier anomalía que pueda ocasionar pérdida o alteración no deseada de información.

Recuerda, más que nunca, que con el trabajo remoto

la seguridad de la información de la Comunidad de Madrid

depende de ti.