CIBERSEGURIDAD

RECOMENDACIONES DE SEGURIDAD PARA EL USO DEL TELETRABAJO

1. Correo electrónico
2. Telefonía móvil
3. Equipos portátiles y comunicaciones
4. Incidentes de seguridad. Comunicación

Recomendaciones facilitadas por la Delegación de Defensa de la CV

RECOMENDACIONES DE SEGURIDAD PARA EL USO DEL TELETRABAJO:

1. Correo electrónico:

- Sea muy cuidadoso con los correos recibidos con información sobre el COVID-19: "Correo de médico de la OMS", "Dominios con mapa de contagios", "Información falsa sobre nuevas infecciones", "archivos PDF con consejos sobre el virus".
- Desconfíe de correos que soliciten donaciones a supuestas víctimas.
- Sospeche de posibles oportunidades de inversión en compañías que afirman poder detectar, prevenir o incluso curar los efectos del virus.
- Malware: aplicaciones o webs maliciosas que ofrecen noticias o mapas interactivos con la expansión de la enfermedad, con el objetivo de robar información sensible, como contraseñas, datos bancarios, contactos, etc . La App más difundida responde al nombre de Corona-Virus·Mop.com, se trata de un troyano.

RECOMENDACIONES DE SEGURIDAD PARA EL USO DEL TELETRABAJO:

- Nunca facilite datos personales ni información de acceso.
- No abra enlace alguno ni descargue ningún fichero adjunto procedente de un correo electrónico que presente cualquier indicio o patrón fuera de lo habitual.
- Antes de abrir cualquier fichero descargado desde el correo, asegúrese de la extensión y no se fíe del icono asociado al mismo.
- No habilite las macros al abrir ficheros adjuntos.
- Nunca trabaje sobre información sensible
- No confíe únicamente en el nombre del remitente. Compruebe que el dominio del correo recibido es de confianza.
- Si un correo procedente de un contacto conocido solicita información inusual contacte por teléfono u otra vía de comunicación para corroborar la legitimidad.
- Elimine los destinatarios incluidos en el mensaje antes de reenviar el correo por motivos de protección de datos.
- Nunca conteste al remitente. Uno de sus objetivos es simplemente confirmar direcciones de e-mail.
- No reenvíe los correos oficiales a sus cuentas de correo particulares.

RECOMENDACIONES DE SEGURIDAD PARA EL USO DEL TELETRABAJO:

2. Telefonía móvil:

- El dispositivo deberá estar actualizado con la última versión del sistema operativo del proveedor oficial del terminal.
- No instale aplicaciones que no provengan de fuentes oficiales o confiables (ej.: Playstore)
- No facilite información personal ni de credenciales de acceso ante una llamada de un supuesto Servicio Técnico .
- Si no está detectando ningún problema en la conexión, no debe recibir ningún tipo de correo o llamada del Servicio Técnico .
- Ante la duda, confirmar el origen de la llamada.

RECOMENDACIONES DE SEGURIDAD PARA EL USO DEL TELETRABAJO:

3. Equipos portátiles y comunicaciones:

- Deberá hacer uso de un equipo configurado con todas las medidas de seguridad que se requerirían a un equipo conectado directamente a la red.
- El equipo deberá tener actualizado el antivirus y las aplicaciones.
- No instale aplicaciones que no provengan de fuentes de confianza.
- Restrinja el uso de dispositivos extraibles como pendrIves, discos duros extraíbles, etc. que no hayan sido verificados por el personal de seguridad del emplazamiento. Estos dispositivos deben ser de uso estrictamente personal y no deben ser compartidos con familiares, compañeros y/o amigos.
- Utilice contraseñas seguras para acceder a sus redes inalámbricas y tenga en cuenta con quien las comparte.

RECOMENDACIONES DE SEGURIDAD PARA EL USO DEL TELETRABAJO:

- Deshabilite las conexiones inalámbricas (Wifi, Bluetooth) mientras no vayan a utilizarse. En lo posible utilice conexiones por cable y únicamente redes wifi privadas, nunca públicas (aeropuertos, cafeterías u otros establecimientos).
- No debe realizar simultáneamente con el mismo equipo actividades ajenas a la actividad de trabajo, como por ejemplo:
  - Acceder a páginas web no relacionadas con la actividad.
  - Ejecutar aplicaciones no corporativas.
  - Abrir documentos recibidos desde fuentes no confiables.
  - Permitir la ejecución de macros de documentos ofimáticos.

4. Incidentes de seguridad. Comunicación:

- Si detecta un incidente de seguridad o tiene la menor sospecha, póngase en contacto con su Jefe de Seguridad