Ministerio del Interior y Seguridad Pública

# CIBERCONSEJOS de Verano

Para organismos e instituciones

## 1. Asegúrate que tus dispositivos y navegadores estén actualizados

Los atacantes son capaces de aprovechar las vulnerabilidades para instalar ransomware y otros malware en dispositivos sin parches. Protege a tu institución manteniendo siempre actualizados los sistemas operativos en computadoras portátiles, teléfonos inteligentes y otros dispositivos que lleves contigo en vacaciones.

## 2. No compartas toda tu información en redes sociales

Antes de salir de vacaciones, además de revisar tus dispositivos y navegadores, revisa el estado de la seguridad de tus redes sociales. Solo una pequeña porción de trabajadores que usa sus redes sociales revisa sus configuraciones de seguridad y privacidad. Eso los expone a ellos y a sus instituciones a un mayor riesgo de estafas a través de phishing, donde los delincuentes pueden utilizar la información de tus viajes para que sus fraudes sean más realistas.

## 3. Precaución con el calor:

El calor es un elemento poco amigo de la tecnología. En estos periodos de altas temperaturas, verifica que en lugares donde tengamos elementos informáticos importantes la temperatura sea adecuada, ya que pueden ser objeto de sufrir altas temperaturas que afecten al correcto funcionamiento o incluso llegar a fallar totalmente.

## 4. Forma adecuadamente a los nuevos miembros de tu equipo de trabajo

Durante el verano nuevas personas se incorporan a los equipos de trabajo, algunos como reemplazos temporales. Procura formar adecuadamente a los nuevos miembros en los planes de ciberseguridad de tu institución, de lo contrario corres riesgo de que no apliquen los procedimientos de seguridad correctos al momento de un incidente.

## 5. Desconéctate del trabajo y de los equipos que no utilizarás

Si en vacaciones te vas a desconectar del trabajo, también practica lo mismo con tus dispositivos. Una vez que determines cuales llevarás contigo en vacaciones, apaga el resto, sin olvidar el PC en tu oficina. Es difícil hackear un dispositivo que no esté disponible, y no servirá de botnet en caso de estar comprometido.

## 6. Los criminales no bajan la guardia. Tampoco lo hagas tú.

Si hay un momento en el que debes encriptar tu computador, tener copias de seguridad en la nube u otro dispositivo, mantener encendido tu firewall, confirmar que tu antivirus y sistemas operativos estén actualizados, utilizar VPN para conectarte y utilizar contraseñas complejas, es precisamente en vacaciones.

## 7. Evita el acceso a redes públicas o desconocidas

Si tienes que acceder a información sensible de tu empresa, hazlo a través de una red privada virtual o VPN. Al hacerlo, siempre usa tus propios dispositivos y nunca accedas a la información corporativa desde una red de uso público. Recuerda cambiar tus contraseñas de acceso en cuanto puedas conectarte a una red confiable.

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática