EQUIPOS PERSONALES

Recuerde mantener las medidas de seguridad:

- Deshabilite la sincronización de su dispositivo con "la nube" cuando no sea necesario.
- Nunca permita que el navegador guarde o recuerde sus credenciales de acceso institucional.
- Desactive la opción de auto-completado de formularios en los navegadores
- Establezca en su dispositivo móvil una clave de acceso y la opción de bloqueo automático.
- Diferencie las contraseñas de acceso al entorno personal y al profesional.
- Evite utilizar sitios no oficiales para descargar las aplicaciones que quiera instalar en su móvil. No utilice aplicaciones ilegítimas en ninguno de tus dispositivos.
- Nunca deje sus equipos desatendidos en lugares públicos o en tu vehículo. Póngalos también a salvo de accidentes.
- El traer sus propios equipos al lugar de trabajo, conlleva los RIESGOS al propietario, como pérdida, robo, ruptura y el acceso a información propensa a virus informáticos, para evitar estos riesgos es recomendable adoptar unas pautas de seguridad CUANDO UTILICEMOS EL DISPOSITIVO MÓVIL.

- En este entorno se debe DIFERENCIAR claramente el correo personal del correo profesional.
- El CIFRADO DE LAS CONEXIONES (por VPN) para el acceso a la información institucional, es una de las

UCR

EQUIPOS PERSONALES

Recuerde mantener las medidas de seguridad:

- Deshabilite la sincronización de su dispositivo con "la nube" cuando no sea necesario.
- Nunca permita que el navegador guarde o recuerde sus credenciales de acceso institucional.
- Desactive la opción de auto-completado de formularios en los navegadores
- Establezca en su dispositivo móvil una clave de acceso y la opción de bloqueo automático.
- Diferencie las contraseñas de acceso al entorno personal y al profesional.
- Evite utilizar sitios no oficiales para descargar las aplicaciones que quiera instalar en su móvil. No utilice aplicaciones ilegítimas en ninguno de tus dispositivos.
- Nunca deje sus equipos desatendidos en lugares públicos o en tu vehículo. Póngalos también a salvo de accidentes.
- El traer sus propios equipos al lugar de trabajo, conlleva los RIESGOS al propietario, como pérdida, robo, ruptura y el acceso a información propensa a virus informáticos, para evitar estos riesgos es recomendable adoptar unas pautas de seguridad CUANDO UTILICEMOS EL DISPOSITIVO MÓVIL.

- En este entorno se debe DIFERENCIAR claramente el correo personal del correo profesional.
- El CIFRADO DE LAS CONEXIONES (por VPN) para el acceso a la información institucional, es una de las

UCR

medidas más eficaces a la hora de proteger la información cuando los dispositivos se utilizan fuera de la red institucional, como por ejemplo Teletrabajo, entre otros.

- EVITE EL USO DE REDES WIFI PÚBLICAS, especialmente si va a manejar información sensible, acceder a cuentas bancarias, etc.
- Haga uso del modo de NAVEGACIÓN DE INCÓGNITO que incluye la mayoría de los navegadores.
- Mantenga el sistema operativo y todas sus aplicaciones ACTUALIZADAS.

central 2511-5000
ci5000@ucr.ac.cr
www.facebook.com/ciucr/
twitter.com/ciucr
CI
Centro de
Informática

medidas más eficaces a la hora de proteger la información cuando los dispositivos se utilizan fuera de la red institucional, como por ejemplo Teletrabajo, entre otros.

- EVITE EL USO DE REDES WIFI PÚBLICAS, especialmente si va a manejar información sensible, acceder a cuentas bancarias, etc.
- Haga uso del modo de NAVEGACIÓN DE INCÓGNITO que incluye la mayoría de los navegadores.
- Mantenga el sistema operativo y todas sus aplicaciones ACTUALIZADAS.

central 2511-5000
ci5000@ucr.ac.cr
www.facebook.com/ciucr/
twitter.com/ciucr
CI
Centro de
Informática