SEGURIDAD EN REDES SOCIALES

BUENAS PRÁCTICAS:

Evite bromas o comentarios inadecuados que puedan traer consecuencias a nivel personal y profesional.

Configure su privacidad con las opciones que ofrecen las redes sociales.

Desactive las funciones de geo-localización cuando sea posible.

Evite reutilizar contraseñas de acceso a los recursos institucionales para acceder a las redes sociales.

Evite emitir valoraciones personales en nombre de la Institución.

PRESENCIA EN LAS REDES SOCIALES:

La forma más común de infección es mediante archivos adjuntos o compartidos a través de correos electrónicos no solicitados o al accesar vínculos que aseguran provenir de entidades bancarias o de empresas de mensajería.

PRECAUCIONES:

- **Conozca bien las condiciones y usos de la red social en la que desea tener un perfil o cuenta.**
- **Sea cuidadoso con la información personal que se agrega, ya que puede ser pública.**
- **Oculte lo mejor posible la información de contacto.**
- **Sea discreto, publicando la menor cantidad de información personal.**

UCR

- Seleccione bien los "amigos" que se aceptan y los que se siguen.
- Realice una minuciosa configuración de las opciones de privacidad de manera precisa para configurar su cuenta.
- Proteja los álbumes de fotos y videos para tener un mayor control de quién puede ver el contenido.
- Evite compartir contenidos de terceros si no está seguro de la veracidad de la información.
- Tenga cuidado con lo que escribe. Evite bromas o comentarios inadecuados que pueden traer consecuencias a nivel personal y profesional.
- Haga un uso responsable y/o profesional de las redes, dado que pueden generar consecuencias en la vida personal, familiar y hasta laboral, suya o de los demás.
- Esté atento ante comportamientos extraños.

RIESGOS:

El uso de redes sociales en entornos institucionales pueden derivar riesgos como la fuga de información de la entidad así como la responsabilización de la Institución por actitudes impropias de su personal.

Evite **PUBLICAR INFORMACIÓN** institucional o empresarial que pueda comprometer la seguridad de su entidad.

Evite mezclar contactos profesionales y personales. Recuerde que no puede controlar lo que ellos pueden escribir sobre usted.

Tenga cuidado al emitir **JUICIOS DE VALOR** a nivel personal sobre temas que atañen a su entidad, ya que estos afectan no solo su prestigio sino también el de la Institución.

Evite poner el **CORREO INSTITUCIONAL** para unirse a una red social. En esos casos utilice su correo electrónico personal.

No brinde **INFORMACIÓN CONFIDECIAL** sobre su trabajo a terceros.

Tenga cuidado con la información que revela sobre su **LUGAR DE TRABAJO** como fotografías, direcciones y otros.

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