

TRATAMIENTO DE LA INFORMACIÓN DIGITAL Y FÍSICA



- Instale y mantenga actualizado un anti-virus y anti-spyware en todos los equipos utilizados en la Institución.



- Utilice redes inalámbricas conocidas, como las redes de trabajo y del hogar.



- Instale periódicamente parches de seguridad y actualizaciones de los sistemas operativos y aplicaciones, estos son constantemente facilitados por los proveedores de los diversos sistemas operativos y de aplicaciones para corregir vulnerabilidades encontradas en sus productos.



- Cree contraseñas seguras y robustas utilizando mayúsculas, minúsculas, números y caracteres especiales (\$&#%).



- Evite repetir contraseñas utilizadas anteriormente y modifíquelas periódicamente, dándoles un uso responsable y adecuado.



- Evite contestar y reenviar correos aparentemente maliciosos, ya que podría poner en riesgo a otras personas o dispositivos, comunique la situación inmediatamente por medio del correo abuse@ucr.ac.cr al Centro de Informática.



- Controle el acceso físico a equipos y componentes de la RedUCR. No se debe permitir que personas no autorizadas tengan acceso físico a equipos y a la administración de sistemas institucionales. Controle el acceso de personas externas encargadas de realizar labores de actualización o reparación des equipos propiedad de la Universidad.



- Evite hacer clic en las ventanas emergentes y en anuncios con información sobre el rendimiento de su computadora.



- Procure usar perfiles de usuario para limitar la posibilidad de instalar programas no autorizados o de dudosa procedencia en equipos personales o de trabajo.



- Desarrolle conciencia y cultura entre los funcionarios y estudiantes sobre los principios básicos de seguridad.



- Realice de forma periódica copias o respaldos de la información más relevante de su trabajo. Estos respaldos son de gran importancia ya que los dispositivos de almacenamiento podrían fallar en cualquier momento por varias razones: errores de los empleados, equipos obsoletos o programas maliciosos que pueden destruir o alterar los datos.