Para evitar que la información de los usuarios sea sustraída, dañada o alterada; y a la vez impedir que puedan ingresar intrusos a nuestra Infraestructura Tecnológica Institucional, les damos algunas pautas que se deben tener en consideración al utilizar los recursos tecnológicos que provee la Universidad para el desarrollo laboral del personal Administrativo y Docentes.

Las pautas son las siguientes:

1. **Cambiar periódicamente la Contraseña:** Esto ayuda a que su contraseña no sea fácil de capturar y si alguien pudo obtenerla, no podrá acceder después de cambiarla. En caso de que se percate que alguien ha estado enviando correo electrónico desde su cuenta, se recomienda cambiar la contraseña lo antes posible y comunicar al Departamento del Centro de Cómputo.

2. **Acceder solo desde computadoras confiables:** En lo posible evitar el uso de computadoras que son destinadas para el uso público, los mismos que podrían tener instalado algún tipo de programa que rastree las pulsaciones de teclas y de esa manera apropiarse de su contraseña.

3. **Cerrar sesión de su correo electrónico:** Es recomendable cerrar sesión cada vez que haya terminado de enviar o leer algún correo electrónico. También es muy recomendable evitar navegar mientras se tiene la sesión de correo abierta, ciertos sitios web pueden capturar los datos de su cuenta.

4. **No grabar contraseñas:** No se debe grabar o guardar las contraseñas en los navegadores (Chrome, Firefox, otros), ni seleccionar la opción de **"Mantener sesión abierta",** para evitar que terceras personas puedan acceder a su cuenta de correo electrónico.

5. **Utilizar contraseñas seguras:** Es recomendable que se tenga una contraseña segura, indescifrable pero fácil de recordar, que contenga números, símbolos y combinación de mayúsculas y minúsculas.

6. **No utilizar las mismas contraseñas:** Se debe evitar usar las mismas contraseñas para el correo electrónico institucional, correo personal, usuario del equipo de cómputo o en sitios webs de índole de entretenimiento o de información que no estén relacionados con las actividades de la institución.

7. **No abrir archivos adjuntos de remitentes desconocidos**: Mediante este mecanismo se puede infectar su máquina, esto hace posible que su computador sea utilizado para captura de información y envió de spam entre otras cosas.

8. **No entregar credenciales de usuario:** No se debe entregar credenciales de usuarios (usuario y contraseña) de equipos de cómputo, de red y correo electrónico institucional a terceras personal, sean estas pertenecientes o NO a la Institución.

9. **Sea cuidadoso con la información que brinda:** no entregue datos personales ni contraseñas vía correo electrónico.
   Aquí una lista de los asuntos más comunes utilizados en el robo de información:
   - ✓ Inconvenientes de carácter técnico
   - ✓ Nuevas recomendaciones de seguridad para prevención de fraudes
   - ✓ Cambios de políticas de seguridad
   - ✓ Inminente desactivación del servicio
   - ✓ Nuevas ofertas de empleos

10. **Analice periódicamente todos los medios de almacenamiento**: Tenga en cuenta que las Memorias USB son actualmente uno de los principales medios de contagios de malware y virus.

11. **Tenga cautela en el uso del Internet:** No se debe descargar archivos de dudosa procedencia, la descarga de juegos, películas y aplicaciones (gratis) supone un riesgo potencial para el buen funcionamiento de su computadora y por ende para su información.

12. **Utilización de software Antivirus:** Se debe utilizar Software Antivirus en los equipos móviles **personales** (laptops, celulares, otros), para evitar la infección de virus informáticos que puedan dañar la información contenida en los mismos o sustracción de datos personales.

13. **Evitar dejar sesiones abiertas del computador:** Se debe evitar dejar abierta las sesiones de usuario de red o del computador, por lo tanto, deberá cerrar la sesión de usuario o bloquear el equipo de cómputo si tiene que ausentarse por momentos cortos o largos de su lugar de trabajo.

14. **Evitar registrarse en sitios web:** Procurar no registrarse en sitios web donde se requiera autenticación de usuario, debido a que podrían ser sitios webs no seguros.

15. **Realizar respaldos de información:** Se deben realizar respaldos de información periódicamente en medios de almacenamiento.