

## Correo Electrónico



No accedas a los **enlaces** en los correos electrónicos, tweets, publicaciones y anuncios en línea que te parezcan **sospechosos**, aún si conoces al remitente.



Si recibes un **correo desconocido** en donde se solicite el **cambio de contraseña** de tu cuenta Uniandes, **repórtalo** de inmediato a [servicioalclientsit@uniandes.edu.co](mailto:servicioalclientsit@uniandes.edu.co).



No abras **correos de remitentes desconocidos** o con **archivos adjuntos sospechosos**, si recibes un correo extraño, remítelo a: [servicioalclientsit@uniandes.edu.co](mailto:servicioalclientsit@uniandes.edu.co)



Utiliza **contraseñas únicas** para cada cuenta, no utilices la misma contraseña de tu cuenta Uniandes, para tu cuenta de Instagram, Facebook o Twitter.



Recuerda utilizar mecanismos que te ayuden a **validar tu identidad** en las plataformas de la Universidad. Hoy utilizamos **A2P**, para más información visita el sitio web <https://cuenta.uniandes.edu.co/Cuenta2/informacionA2P.jsp>



No ingreses tu **información sensible**, como la contraseña Uniandes o la clave de tu cuenta bancaria, en enlaces provenientes de **cadena de redes sociales o de WhatsApp**, recuerda que ninguna institución te solicitará este tipo de información por canales de comunicación no oficiales.



Bloquea aquellos **correos no deseados** que contienen información que no es de tu interés, para mayor información te enseñamos como hacerlo en este [video](#).



## Teléfono Celular



Para proteger la información que almacenas en tu celular debes mantener todas las apps **actualizadas** en las versiones más recientes. Recuerda descargarlas **únicamente de los sitios oficiales**. Por ejemplo la Play store o la Apple store.



Tu teléfono móvil trae una **contraseña por defecto** para activar la "ZONA WIFI" y compartir tus datos. Para evitar que **personas desconocidas se conecten a tu celular**, es mejor cambiarla por una contraseña que incluya letras mayúsculas, minúsculas, números y caracteres especiales que la hagan más robusta y **difícil de conocer**.



En las **configuraciones de seguridad** de tus aplicaciones móviles puedes **desactivar tu ubicación** y así evitar que todos conozcan en dónde te encuentras e incluso que tus redes se inunden de publicidad no deseada. Si quieres conocer más sobre éste tema pulsa [aquí](#).



No compartas ni difundas cadenas de WhatsApp en donde te ofrezcan **beneficios**, subsidios, donativos entre otros, a cambio de tu **información**.