

Desde el eje de Seguridad queremos invitarte a que no seas víctima de ingeniería social, por eso te recomendamos lo siguiente:

No abras correos de origen desconocido, elimínalos inmediatamente.



No contestes nunca los mensajes que creas que son sospechosos.

Verifica la seguridad de los sitios web en los que introduzcas datos personales.



Cuidado con los enlaces recibidos por email, SMS, whatsapp o redes sociales.

Cuidado con los archivos adjuntos del email, SMS, whatsapp o redes sociales.

Ten siempre actualizado el sistema operativo y el antivirus, así como activado.

Escribe la URL de forma manual y no uses los enlaces de los mensajes sospechosos.

Verifica la seguridad de las redes wifi-públicas en las que te conectas.

Recuerda: el protagonista de la Política de Seguridad de la Información eres tú.