

CORREO ELECTRÓNICO

1 Uso institucional

Esta cuenta es solo para el desarrollo de las funciones de nuestro puesto, somos responsables de su uso y no debe usarse para fines personales o de otro tipo.

2 Contraseña segura

NO debemos compartirla con nadie, en caso de que se debiera hacer, se debe cambiar lo antes posible.

Debe cambiarse con regularidad.

Debe contener letras en mayúsculas, minúsculas, números y algún símbolo.

Se puede usar una frase con algún número y símbolo al final y es fácil de recordar y difícil de descifrar debido al número de caracteres.

3 Phishing

Se debe evitar dar clic en los correos que tienen enlaces dentro de su mensaje y de los cuales no tengamos conocimiento previo de a donde lleva dicho enlace.

5 Evita revisar tu correo en Wi-Fi públicas

Muchas de las redes públicas no tienen seguridad o es muy básica, es relativamente fácil que personas puedan ingresar para robar tu información.

4

No descargar archivos adjuntos

Si no conoces al remitente o desconfías del cuerpo de un correo.

6 No registres tu correo en cualquier sitio

Podrían hacer mal uso de él o dejarlo en bases de datos de donde cualquiera podría tomarlo y enviar correos maliciosos y no deseados.

7 No enviar información de usuarios y contraseñas por correo.

Si fuera necesario hacerlo, se debe cambiar la contraseña en cuanto sea posible.

8 Cerrar las sesiones que abramos.

Si se abre el correo en un equipo que no es nuestro, debemos asegurarnos de cerrar la sesión.