60 Anos Setronix desde 1966

OCTUBRE 2026

2.ª QUINCENA | PREVENCIÓN



CIBERSEGURIDAD
PARE Y CONFIRME

Un mensaje urgente no exime de la verificación.

1. Peligros y riesgos

Peligros: Mensajes falsos, adjuntos y enlaces sospechosos.

Riesgos: Robo de datos, fraude y acceso indebido a cuentas.

2. Antes de empezar

- Vea la dirección completa del remitente.
- Confirme los pedidos por un contacto ya conocido.
- Use solo aplicaciones y canales autorizados.

3. Pare y comunique

- Solicitud de contraseña o código de acceso.
- Urgencia, secreto o cambio de datos bancarios.
- ¿Ya hizo clic o envió datos? Comunique de inmediato.

4. Cómo actuar: cuatro pasos para prevenir

1



Lea

Verifique remitente y contexto.

2



Confirme

Use un contacto independiente.

3



Proteja

No comparta credenciales ni códigos.

4



Comunique

Informe por el canal interno aplicable.

5. Elija la medida adecuada a la situación

Situación	Medida preventiva
Email / SMS	No abra adjuntos ni enlaces cuyo origen no haya confirmado.
Solicitudes de pago	Valide los cambios por otro canal ya conocido.
Cuentas / credenciales	Use contraseñas únicas; active MFA cuando esté disponible.
Posible incidente	Guarde el mensaje; siga las instrucciones de soporte técnico.

Buenas prácticas: No se fíe solo del nombre mostrado ni del aspecto del mensaje. La autenticación multifactor (MFA) refuerza la protección; nunca comparta los códigos correspondientes.

6. ACCIÓN DE LA QUINCENA En el próximo mensaje inesperado, confirme el origen antes de hacer clic. Identifique el canal interno para comunicar una sospecha.

LEA • CONFIRME • PROTEJA • COMUNIQUE

CNCS: buenas prácticas CNCS: contraseñas