



CHECKLIST DE SEÑALES DE VULNERABILIDAD

INDICADORES DE VULNERABILIDAD DIGITAL:

Dificultades digitales básicas



- ☐ Le cuesta mucho saber si un mensaje es real o falso.
- ☐ No sabe qué hacer cuando recibe un SMS; correo o llamada extraña.
- ☐ Tiene miedo de utilizar el teléfono móvil o el ordenador.

Comportamientos de riesgo



- ☐ Hace clic en cualquier enlace sin pensar.
- ☐ Da información personal con facilidad.
- ☐ Acepta ayuda de desconocidos para "hacer gestiones".

Señales emocionales



- ☐ Se pone nervioso/a cuando recibe mensajes o llamadas.
- ☐ Tiene vergüenza de decir que no entiende alguna cosa.
- ☐ Está asustado/da y dice "me pueden engañar".

Situaciones que preocupan



- ☐ Ha recibido muchos mensajes sospechosos últimamente.
- ☐ Ha perdido dinero o no sabe explicar algún pago.
- ☐ Tiene movimientos extraños en la cuenta o tarjeta.

Riesgo inmediato



- ☐ Ha dado la contraseña, códigos o fotos del DNI.
- ☐ Ha realizado un pago o transferencia que no tocaba.
- ☐ Ha instalado una aplicación que no reconoce.

COMO USARLO:

- ☒ 1 o 2 señales: Atención suave → dar consejos y revisar dudas.
- ☒ 3 o 4 señales: Vulnerabilidad clara → activación de circuito preventivo.
- ☒ Cualquier señal de riesgo inmediata: Acción urgente. Llamar a la policía.



CIRCUITOS

CIRCUITO 1



Quando recibe un mensaje sospechoso (no ha hecho nada)

LA PERSONA RECIBE UN MENSAJE EXTRAÑO



EXPLICAR EL CASO AL/LA PROFESIONAL



EL/LA PROFESIONAL ESCUCHA Y TRANQUILIZA



REVISA EL MENSAJE CON LA PERSONA
(WhatsApp / SMS / Correo / Llamada)



ES UNA ESTAFA? —► **NO**



SÍ



ACCIÓN:

- Bloquear el número/correo
- Borrar el mensaje
- No contestar



EXPLICAR CÓMO DETECTAR FUTURAS ESTAFAS



ACOMPAÑAMIENTO BREVE

“Si tienes dudas, tráemelo antes de hacer nada.”



FIN DEL CIRCUITO

CIRCUITO 2



Ha contestado, pero NO ha dado datos

LA PERSONA HA RESPONDIDO A UN MENSAJE



ESTÁ PREOCUPADA Y LO EXPLICA



EL/LA PROFESIONAL CALMA:
"Estás a tiempo de pararlo."



REVISAR QUÉ HA HECHO:

- ¿Hizo clic?
- ¿Abrió algún enlace?
- ¿Escribió alguna respuesta?



ACCIÓN:

- Bloquear el contacto
- Cambiar contraseñas básicas
- Revisar Apps extrañas



ACOMPANIAMIENTO:

"Ven mañana para asegurarnos de que todo está bien."



DERIVACIÓN SI HACE FALTA:

- Dinamizador/a TIC
- Familiares o persona de confianza



FIN DEL CIRCUITO

CIRCUITO 3



Ha dado datos, códigos o dinero

LA PERSONA HA DADO DATOS / CÓDIGOS / DINERO



LA PERSONA ESTÁ ANGUSTIADA O AVERGONZADA



EL/LA PROFESIONAL TRANQUILIZA:

“No es culpa tuya. Lo arreglaremos paso a paso.”



PREGUNTAR QUÉ HA ENTREGADO EXACTAMENTE:

- Datos personales?
- Contraseñas?
- Tarjeta bancaria?
- Códigos por SMS?
- Transferencias?



ACCIONES URGENTES:

SI HAY DATOS DEL BANCO:

→ Orientarla para que llame al banco o vaya a la sucursal para bloquear tarjeta/cuenta.

SI HAY CONTRASEÑAS:

→ Cambiar contraseñas inmediatamente.
→ Activar la verificación en dos pasos.

SI HA PERDIDO DINERO:

→ Recoger información
→ Orientar hacia la denuncia (Policía). Indicarle que no borre mensajes ni ninguna evidencia.



ACOMPANIAMIENTO ACTIVO:

“Te ayudo a hacer la llamada o a preparar la denuncia.”



SEGUIMIENTO:

Revisar en los días siguientes si todo continúa seguro.



FIN DEL CIRCUITO

CIRCUITO 4



Cuando el riesgo no es claro (situación difusa)

MENSAJE / LLAMADA / SITUACIÓN AMBIGUA



EL/LA PROFESIONAL ESCUCHA Y OBSERVA



FORMULAR 3 PREGUNTAS CLAVE:

1. ¿Te pedían dinero?
2. ¿Te pedían datos?
3. ¿Te hicieron sentir prisa?



SI ALGUNA ES "SÍ" → TRATAR COMO RIESGO MEDIO/ALTO



SI TODO ES "NO" → probablemente no es estafa



ACCIÓN:

- Explicar precauciones
- Recomendar no responder
- Revisar futuros mensajes



FIN DEL CIRCUITO

CIRCUITO 5



Acompañamiento emocional (transversal a todos)

PERSONA ASUSTADA / AVERGONZADA



EL/LA PROFESIONAL ACOGE:

"Es normal sentirse así."
"No estás solo/a."



NORMALIZAR:

"A mucha gente le pasa."



MARCAR CONTROL:

"Lo revisaremos juntos/as y lo podemos arreglar."



ACOMPANIAMIENTO:

Ofrecer ayuda para llamar, revisar, denunciar.



SEGUIMIENTO SUAVE:

"Si te sientes mal, ven y lo hablamos."



FIN DEL CIRCUITO

SCRIPT DE PRIMERA ACOGIDA

SI LA PERSONA MAYOR EXPRESA DUDAS O SOSPECHA DE ESTAFA

OBJETIVO

Escuchar, validar, reducir la angustia y obtener información básica para valorar el riesgo.

1 ACOGIDA Y VALIDACIÓN

"Entiendo que esto te preocupa. Gracias por explicármelo. Aquí estás en un espacio seguro y veremos juntos qué ha pasado."

2 PREGUNTA ABIERTA PARA SITUAR EL CASO

"¿Me puedes contar qué ha pasado paso a paso? ¿Cuándo lo recibiste y qué te hizo sospechar?"

3 RECOGIDA MÍNIMA DE INFORMACIÓN (SIN HACER SENTIR INTERROGADA A LA PERSONA)

¿Qué canal fue? (teléfono, SMS, WhatsApp, correo, redes...)

¿Qué pedían? (datos, dinero, clics, contraseña...)

¿Sabes si llegaste a hacer clic/enviar algo?

4 TRANQUILIZAR Y NORMALIZAR

"Cada vez hay más casos como este. No es tu culpa: estos fraudes están hechos expresamente para engañar y son muy convincentes."

5 PRIMER CONSEJO DE SEGURIDAD

"Lo más importante ahora mismo es no responder y no hacer clic en nada más."

6 DERIVACIÓN O SEGUIMIENTO

"Si te parece, revisemos juntos qué puedes hacer ahora mismo para protegerte, y si es necesario te ayudo a contactar con los servicios de apoyo correspondientes."

SCRIPT PARA PERSONAS MAYORES

QUE NO ESTÁN SEGURAS DE SI HAN SIDO VÍCTIMAS

OBJETIVO

Resolver dudas sin hacer que la persona se sienta ignorante.

"Es muy buena idea consultarlo. A veces no es fácil distinguir si es una estafa o no, y preguntar es la mejor manera de prevenir."

"¿Me explicarías qué recibiste o qué te pidieron? Así podré orientarte sobre si existe un riesgo real."

SI PARECE UNA ESTAFA:

"Entiendo la confusión: estas estafas están diseñadas para parecer reales. Te propongo dar el paso X (bloquear, denunciar, revisar movimientos...). Te acompaño en ello."

SI NO PARECE UNA ESTAFA:

"Por lo que me explicas, no parece un caso de riesgo, pero has hecho muy bien en preguntar. Siempre es una buena práctica comprobarlo."

SCRIPT CUANDO LA PERSONA ESTÁ

MUY ANGUSTIADA O AVERGONZADA

OBJETIVO

Reducir el impacto emocional, evitar la culpa y ofrecer apoyo.

"Es normal que te sientas así. Estas situaciones pueden generar mucha angustia, pero no estás solo/a. Estamos aquí para ayudarte."

"A cualquiera le puede pasar. Además, estas estafas están pensadas para presionar y confundir. Lo importante ahora es qué hacemos a partir de este momento, y te acompañaré en el proceso."

"Si te parece, respiramos un momento juntos/as y lo revisamos con calma."

SCRIPT DE DETECCIÓN PROACTIVA (CUANDO EL/LA PROFESIONAL VE INDICIOS)

OBJETIVO

Abrir conversación sin señalar ni juzgar.

"Estamos viendo muchos casos de llamadas y mensajes sospechosos estos días. ¿Has recibido algo raro últimamente?"

"A veces parece que es del banco o de Correos, pero puede ser una estafa. Si alguna vez tienes dudas, nos lo puedes comentar sin ningún problema."

"Hace poco hemos ayudado a otras personas a las que les pasó algo parecido, así que si necesitas revisar algo, lo hacemos juntos/as."

SCRIPT CUANDO LA PERSONA ADMITE QUE HA DADO DATOS O DINERO

OBJETIVO

No culpabilizar, recoger información clave y activar medidas.

"Gracias por contármelo y por confiar en mí. Es más habitual de lo que parece, y has hecho muy bien en decirlo."

"Para poder ayudarte, ¿puedo preguntarte qué llegaste a compartir o enviar? (datos personales, datos bancarios, códigos, dinero, contraseñas...)"

"Con lo que me explicas, lo más recomendable es hacer estos pasos: ... Si quieres, los hacemos juntos/as."

"Es importante que no te culpes. Lo que importa es que hemos reaccionado a tiempo."

SCRIPT PARA REFORZAR EMPODERAMIENTO Y PREVENCIÓN AL FINAL DE LA CONVERSACIÓN

OBJETIVO

Reforzar el empoderamiento, consolidar pautas de prevención y promover la consulta antes de actuar.

“Recuerda que no tienes que hacer nada que no tenga sentido o que te presione. Tienes derecho a parar la conversación, colgar o pedir ayuda.”

“Lo más importante es que, si tienes cualquier duda, antes de iniciar cualquier trámite nos lo consultes. Esa es la mejor protección.”

“Si quieres, puedo darte algunos consejos prácticos para que no te vuelva a pasar y para que te sientas más seguro/a.”



PARA
PÁRATE. RESPIRA. NO HAGAS CLIC.

PIENSA

¿ESTA PERSONA TE PIDE DINERO O INFORMACIÓN?

VERIFICA

ENSEÑA EL MENSAJE A ALGUIEN ANTES DE HACER NADA



PARA

AYUDA A LA PERSONA A FRENAR EL IMPULSO DE ACTUAR SIN PENSAR.

PIENSA

HACEROS JUNTOS 3 PREGUNTAS:

- **¿PIDE DATOS?**
- **¿PIDE DINERO?**
- **¿TIENES SENSACIÓN DE PRISA O MIEDO?**

VERIFICA

COMPROBAD JUNTOS LA INFORMACIÓN ANTES DE RESPONDER.

PARA NO HAGAS CLIC. NO RESPONDAS. NO PAQUES.

SI TE LLEGA UN MENSAJE EXTRAÑO, PARA.

LAS ESTAFAS SIEMPRE QUIEREN QUE HAGAS LAS COSAS RÁPIDO.

TIENES DERECHO A TOMARTE TU TIEMPO.

RECORDATORIO CLAVE:

“CUANDO TIENES PRISA, ES MÁS FÁCIL QUE TE ENGAÑEN.”

PIENSA ¿QUÉ ME PIDEN? ¿POR QUÉ TANTA PRISA?

¿TE PIDEN DINERO?

¿TE PIDEN DATOS O CONTRASEÑAS?

¿TE HACEN SENTIR MIEDO, PRISA O CULPA?

¿TE DICEN QUE “SI NO LO HACES AHORA, HABRÁ PROBLEMAS”?

SI ALGUNA RESPUESTA ES “SÍ”:

ES MUY PROBABLE QUE SEA UNA ESTAFA.

VERIFICA PREGUNTA A ALGUIEN DE CONFIANZA. NOS LO PUEDES ENSEÑAR.

ENSEÑA EL MENSAJE A ALGUIEN DEL CASAL, BIBLIOTECA O CENTRO.

LLAMA TÚ MISMO AL BANCO, A CORREOS O A QUIÉN SEA.

BUSCA EL TELÉFONO REAL (NO EL DEL MENSAJE).

SI TIENES DUDAS: MEJOR NO HACER NADA ANTES DE VERIFICAR.

RECORDATORIO CLAVE:

“ENSEÑAR UN MENSAJE A ALGUIEN ES LA MEJOR PROTECCIÓN.”