

eÁ  
espazoAxil

---



fundación **esplai**



XUNTA  
DE GALICIA

CONSELLERÍA DE  
POLÍTICA SOCIAL  
E IGUALDADE

# CIBERSEGURIDAD PRÁCTICA

Para entidades del Tercer Sector  
y la Economía Social

---

Sesión básica, directa y aplicable desde mañana

Jesús Velasco | 18 de septiembre de 2026 | 90 min



## NUESTRA META

# Salir con cinco decisiones claras

Conocer, proteger, verificar, responder y mejorar.



PREGUNTA AL GRUPO

## ¿Qué situación os preocupa más en vuestra entidad?

## CASO CONDUCTOR

# La asociación Brétema tiene buenas intenciones...

...pero depende de hábitos informales.

## Cuenta compartida

Cinco personas conocen la misma contraseña.

## Sin doble factor

El correo solo depende de una contraseña.

## Datos locales

La documentación vive en un portátil.

## Sin protocolo

Nadie sabe a quién avisar ni qué conservar.



## PREGUNTA AL GRUPO

¿Qué podría salir mal primero?

## CONTEXTO

# No protegemos “informática”

Protegemos personas, actividad, confianza e información.

**PERSONAS**

Datos personales,  
participantes, voluntariado

**ACTIVIDAD**

Atención, proyectos, pagos y  
plazos

**CONFIANZA**

Credibilidad ante usuarios y  
financiadores

**INFORMACIÓN**

Expedientes, contratos y  
documentación

**Un incidente pequeño puede convertirse en una interrupción grande si no hay preparación.**

## 1 • CONOCER

# Si no sabemos qué usamos, no podemos protegerlo

Empieza con un inventario mínimo, no con una herramienta compleja.

## EQUIPOS

Portátiles, móviles, NAS,  
USB

## CUENTAS

Correo, banca, nube, redes

## APLICACIONES

Gestión, nóminas, proyectos

## INFORMACIÓN

Qué es sensible y dónde  
está

**Consejo: una hoja sencilla y una persona responsable ya son un comienzo.**

## 2 • PROTEGER

# Una persona, una cuenta, permiso necesarios

Las cuentas compartidas eliminan trazabilidad y complican las bajas.

## Cuenta individual

Podemos saber quién accede y retirar el acceso sin cambiar la contraseña a todo el mundo.

## Menor privilegio

Cada persona accede solo a la información que necesita para su función.

## Alta, cambio y baja

Un procedimiento corto evita accesos olvidados al cambiar o finalizar una colaboración.



## PREGUNTA AL GRUPO

Si alguien se marcha hoy, ¿podéis retirar todos sus accesos?

## 2 • PROTEGER

# El doble factor cambia el resultado

Una contraseña robada deja de ser suficiente por sí sola.

1 Algo que sabes

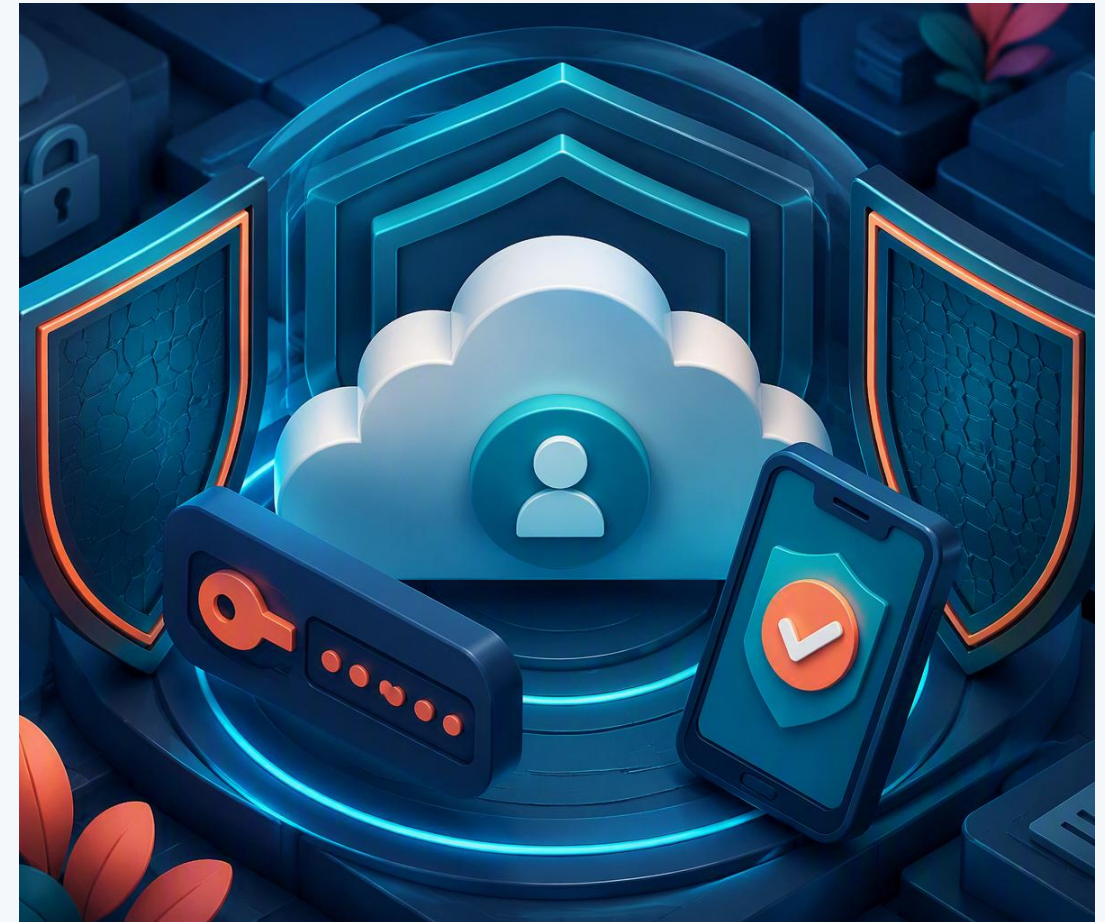


2 Algo que tienes

## PRIORIDAD

**Correo • almacenamiento • banca •  
administración**

**Nunca apruebes una solicitud de acceso que no  
hayas iniciado.**



## PREGUNTA AL GRUPO

**¿En qué cuentas críticas aún no tenéis doble factor?**

# El equipo debe protegerse solo

## Automatize lo que no debería depender de la memoria



## ACTUALIZAR

## Sistema, navegador y aplicaciones

## BLOQUEAR

Automáticamente cuando nos alejamos

**CIFRAR**

### Especialmente portátiles y móviles

## LIMITAR

## No trabajar normalmente como administrador

## 2 • PROTEGER

# Sincronizar no siempre es tener c

La copia debe estar generada con periodicidad y haberse probado

## Guardar bien

Entorno corporativo, carpetas ordenadas y permisos revisados.

## Copiar aparte

Evitar que el único ejemplar viva en un portátil, USB o disco local.

## Probar la recuperación

Una copia que nunca se ha restaurado es una esperanza, no una garantía.

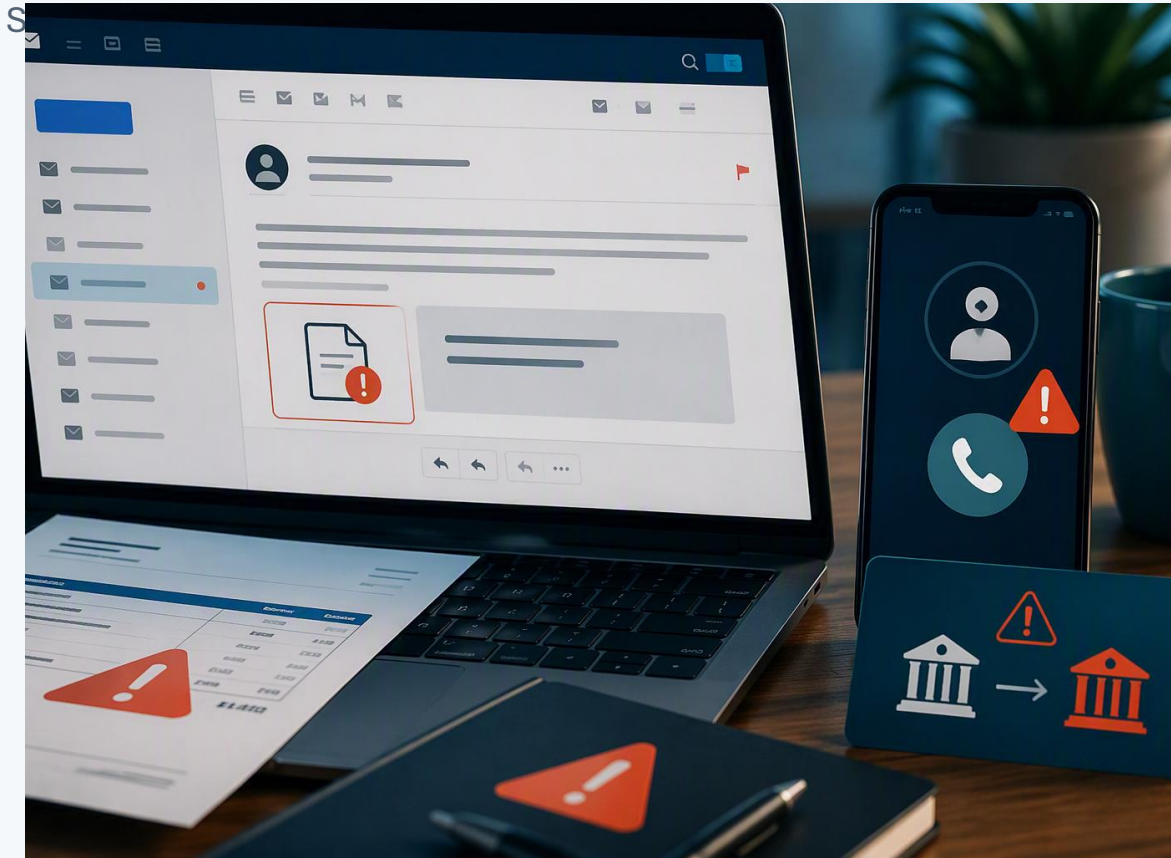


PREGUNTA AL GRUPO

¿Cuándo recuperasteis por última vez una carpeta de prueba?

## 3 • VERIFICAR

# El fraude no tiene que “parecer técnico”



## URGENCIA

“Tiene que ser hoy”

## EXCEPCIÓN

“Esta vez hazlo por este canal”

## CREDENCIALES

“Inicia sesión para comprobarlo”

## DINERO O DATOS

“Cambia la cuenta / envíame el listado”

## EJERCICIO

# “Hemos cambiado de cuenta bancaria”

Un correo plausible. Una decisión que debe verificarse.

Proveedor habitual <facturas@proveedor-ejemplo.com>

## Asunto: Actualización urgente de datos bancarios

Buenos días,

Hemos cambiado de entidad bancaria. Necesitamos que la factura pendiente se abone hoy en la nueva cuenta adjunta. Confirmanos la transferencia cuanto antes.

Gracias.

### 1 • NO RESPONDER

No uses teléfonos ni enlaces incluidos en el mensaje.

### 2 • SEGUNDO CANAL

Llama al contacto conocido o usa un canal ya validado.

**La medida no es “mirarlo mejor”. Es cambiar de canal.**

PREGUNTA AL GRUPO

**¿Qué señales os harían detener el pago?**

SI YA OCURRIÓ

# Pulsar no es el final: callar sí amplifica el daño

Avisar pronto permite contener.



## DETENTE

No sigas introduciendo datos



## AVISA

Comunica qué has hecho y cuándo



## CAMBIA

Credenciales desde un equipo seguro



## REVISA

Sesiones, reglas y actividad con soporte

**Cultura útil: premiar la comunicación temprana, no buscar culpables.**

## ZONAS COTIDIANAS

# Dispositivos personales e inteligencia artificial

La comodidad no elimina la responsabilidad sobre los datos.

## Dispositivo personal

Bloqueo, actualización, separación del uso personal y acceso solo a la información necesaria.

## Herramientas de IA

No introducir datos personales, confidenciales o internos en servicios no autorizados.

## Alternativa práctica

Anonimiza el contenido o utiliza una solución corporativa



PREGUNTA AL GRUPO

¿Pegarías ese documento en una web pública?

## 4 • RESPONDER

# Protocolo PARA

**P** **PARA Y DESCONECTA** En las primeras horas, desconecta de la red si sospechas infección.

**A** **AVISA** Comunica de inmediato a la persona responsable.

**R** **REGISTRA** Qué ocurrió, cuándo y qué información podría estar afectada.

**A** **ACTÚA CON AYUDA** Credenciales seguras, soporte, protección de datos y recuperación.



## AUTOEVALUACIÓN

## Sí • No • No lo sé

“

¿Hay una persona referente?



¿Conocemos equipos, cuentas y servicios?



¿Cada persona tiene cuenta individual?



¿MFA en servicios críticos?



¿Equipos y aplicaciones actualizados?



¿Datos en entorno corporativo?



¿Copias separadas y probadas?



¿Procedimiento de altas y bajas?



¿El equipo reconoce fraudes?



¿Normas para dispositivos e IA?



¿Sabemos a quién avisar?



¿Podemos seguir operando tras un incidente?



## 5 • MEJORAR

# Tres horizontes, no veinte proyectos

P

## MAÑANA

Activar MFA · dejar contraseñas compartidas · actualizar · revisar accesos.

## PRÓXIMOS 30 DÍAS

Ordenar almacenamiento · copias · altas y bajas · capacitación breve.

## PRÓXIMOS 3 MESES

Política básica · revisión de riesgos · registro de incidentes · pruebas periódicas.



PREGUNTA AL GRUPO

**Escribe una acción concreta en cada horizonte.**

## RESUMEN

# Cinco verbos para llevarse

Si se acuerdas una diapositiva, que sea esta.

**1 CONOCER** inventario + responsable

**2 PROTEGER** cuentas + MFA + equipos + copias

**3 VERIFICAR** segundo canal

**4 RESPONDER** protocolo PARA

**5 MEJORAR** mañana + 30 días + 3 meses

**La seguridad mejora cuando las responsabilidades y los hábitos dejan de ser informales.**

# ¿PREGUNTAS?

Recursos para pedir ayuda y actuar con criterio

## INCIBE · 017

Ayuda gratuita y confidencial ante dudas, riesgos e incidentes de seguridad digital. No es un canal de denuncia.

## AEPD · Brechas

Orientación y notificación cuando una brecha de datos personales pueda implicar riesgo para las personas.

## CONTACTOS INTERNOS

Responsable de seguridad · soporte tecnológico · protección de datos · dirección.

**Tu primera llamada debe estar decidida antes del incidente.**

# Cuestionario de avaliación do Ver án Áxil, 18/09/2026

