EL SELLO DE CONFIANZA

SESIÓN 2

Centr@Tec
Servicios Avanzados de Innovación para Pymes

icecyl competitividad empresarial

Junta de Castilla y León

CÓMO CERTIFICAR TUS SERVICIOS PARA EVITARTE LAS SANCIONES.

LA ITV DE LA CIBERSEGURIDAD

Está ocurriendo... PERO AHORA MÁS

1. EL CLIENTE LLEGA
2. EL CLIENTE MIRA
3. EL CLIENTE DUDA
4. EL CLIENTE SE VA

¿Por qué ocurre?

CLIENTES	Competencia	Decisión
Cada vez más exigentes	Más proveedores nacionales /internacionales.	Más Opciones = Paralisis por Analisis

¿Por qué ocurre?

¿Qué hace dudar a tus clientes?

•

¿Os está preocupando lo mismo?

Los dos lados de la moneda...

Unos lo viven como...

Clientes que no vuelven.

Cartas de multas que si llegan.

Redes sociales bloqueadas.

Reseñas terribles en Google.

Nosotros lo vemos en...

Brechas de seguridad.

Servidores caídos.

¿Copias de seguridad? Ninguna.

“¡Arreglalo ya!”

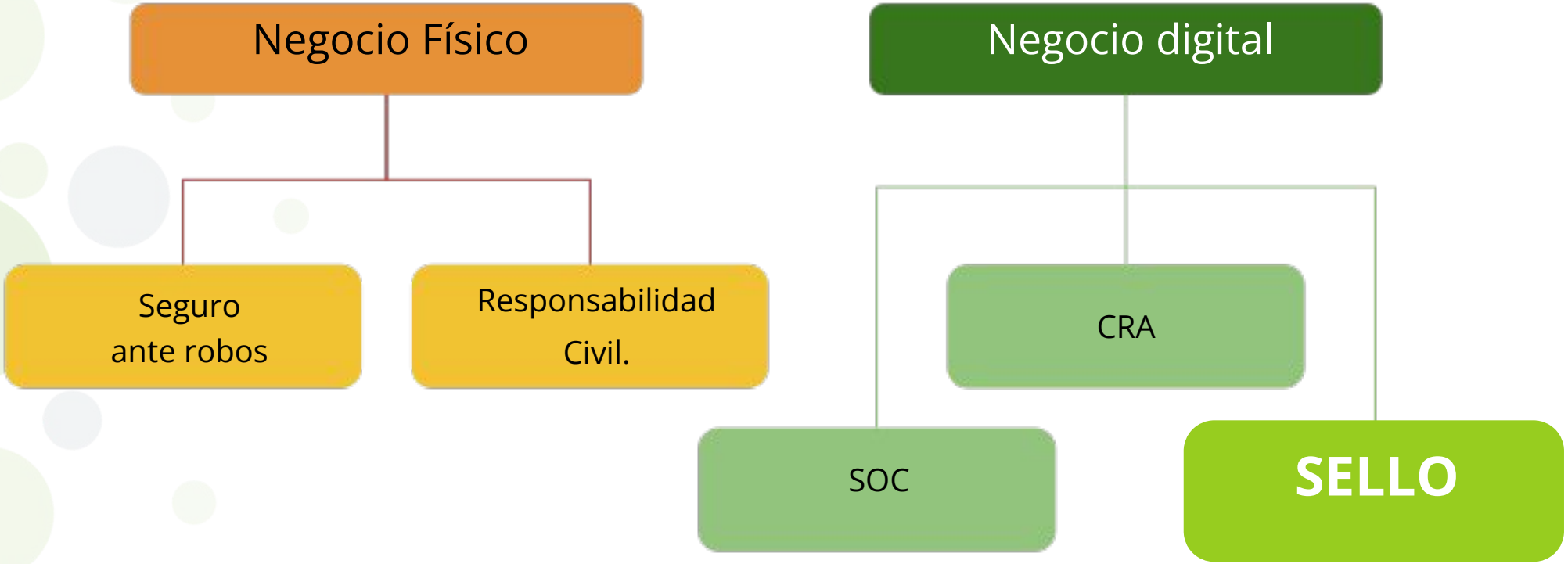
Los dos lados de la moneda...

¿A cuánta gente conocen que ha sufrido un ciberataque?

•

¿Por qué suben más los números de afectados?

No es tan Diferente...

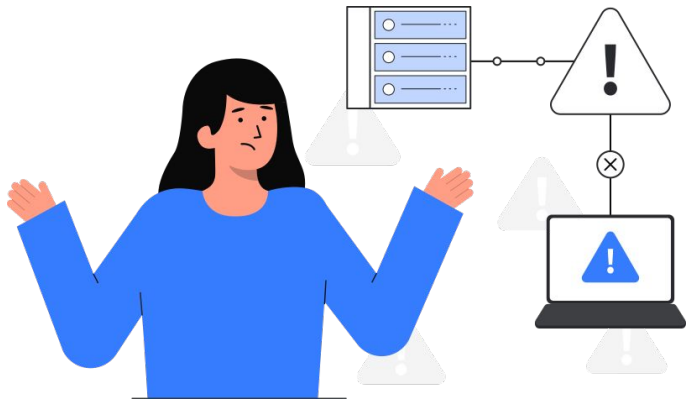


Cuántos tenéis...

¿Antivirus?

¿Alarma en casa?

¿Candado en la bici?



Proteger lo personal es instintivo,

¿Por qué la seguridad digital empresarial parece más una obligación que una satisfacción?

¿Lo es o no lo es?

Un **extintor** ¿Es un gasto o una inversión?

Un **airbag** ¿Es un gasto o una inversión?

Una **barandilla** ¿Es un gasto o una inversión?

•

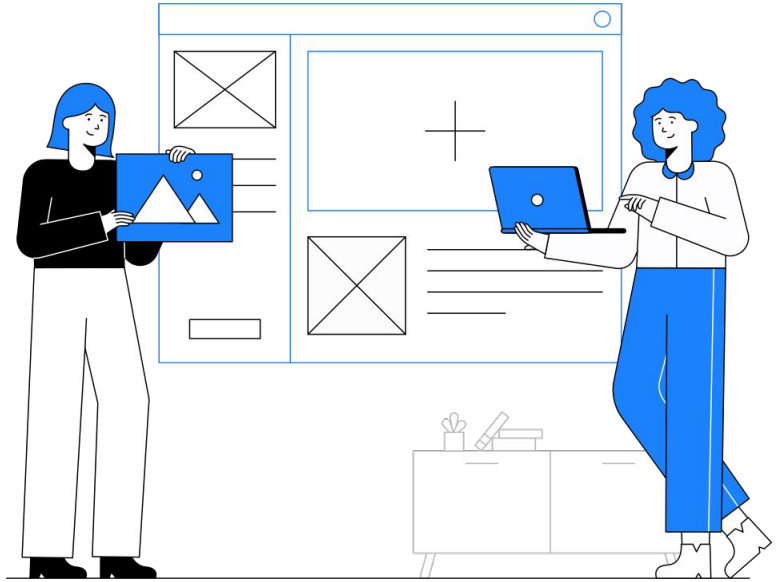
Y ¿ una auditoría o un mapeo
de la salud digital de
tus ordenadores, móviles, servidores...?

¿Qué significa el Sello de Confianza?

El proceso se fundamenta en el ciclo PDCA (Plan-Do-Check-Act) de mejora continua

¿Palabras o Pruebas?

Palabras	Pruebas
Hay que tener mucha confianza para confiar lo que tienes en solo palabras	Un contrato, Un certificado, Una promesa legal.



El Sello de Confianza certifica que tu PYME cumple estándares estrictos de ciberseguridad.
Verificado por expertos, genera confianza con sistemas auditados y normativas como ENS, NIS2 Y RGPD.

¿Qué más significa?

La seguridad no es un estado estático, sino un proceso continuo.

Certificación Visible

Proceso estandarizado de mapeo y auditoría.

Socios / Sinergias

Se exige un Sello para nuevas colaboraciones.

Dentro y Fuera

Cultura, hábitos y decisiones en la empresa.

Evitar Sanciones

Cumplir normativas
p.ej NIS2, CRA, ENS, RGPD

Más Ventas . Mas descanso

No te van a llegar calumnias por culpa
de fallos en tu servicio.

¿Lo es o no lo es?

Es bueno que nos acostumbremos
a hablar de la ENS, NIS2 o el RGPD?

•

¿A quién le suena alguna?

Normativas y Estándares Clave

RGPD	Reglamento General de Protección de Datos, protege la información personal de los clientes, si su empresa opera en la Unión Europea.
NIS2	Los sectores esenciales y digitales deben contar con planes de prevención, respuesta y notificación rápida de ciberincidentes, bajo riesgo de fuertes multas.
ENS (CIDAT*)	Marco español que exige a las administraciones públicas y a sus proveedores garantizar un nivel mínimo y auditable de seguridad en sus sistemas y servicios.
	El ENS contempla 75 medidas de seguridad: Organizativo, operacional, medidas protección
CRA	Nueva regulación europea que exige que cualquier hardware o software “conectado” vendido en la UE sea seguro “por diseño y por defecto”.

*La categorización se basa en cinco dimensiones de seguridad: Confidencialidad [C], Integridad [I], Disponibilidad [D], Autenticidad [A] y Trazabilidad [T]

La parte que no le gusta a nadie...

FASE 01 Advertencias

Requerimientos formales de la AEPD*
para implantar controles y corregir fallos.

FASE 02: MULTAS

- Falta de información clara sobre el tratamiento de datos personales.
- Ausencia de consentimiento explícito para procesar los datos.
- No atender derechos ARCO (acceso, rectificación, cancelación, oposición).
- Sin registro de actividades o DPIA cuando corresponde.
- Medidas de seguridad inadecuadas.
- **No notificar brechas de datos dentro del plazo.**
- No designar DPO cuando es obligatorio.

Agencia española de protección de datos.

ETAPAS
PARA CONSEGUIR
EL SELLO DE CONFIANZA

Estas etapas pueden variar dependiendo de la empresa

Fase 1: Solicitud y Evaluación Preliminar.

- Registro inicial: La empresa completa un formulario con datos y documentación requerida por la entidad certificadora.
- Se entrega información básica sobre el contexto de la organización y los sistemas que se pretenden certificar.
- Se realiza una revisión documental previa (“gap analysis”) para identificar brechas respecto a la norma objetivo
- Se establece el alcance y la categorización de los sistemas según su nivel de criticidad y los impactos potenciales
- La organización debe subsanar las brechas detectadas.

Fase 2: Auditoría y Evaluación

- El equipo auditor revisa exhaustivamente la documentación facilitada para verificación completa.
- Se comprueba comprensión de la organización respecto a los requisitos normativos y posibles no conformidades
- El equipo auditor visita la organización y realiza una auditoría presencial (o combinada con remoto según caso).
- Se verifica, mediante entrevistas, observaciones directas y revisión de evidencias.
- Se revisan sistemas técnicos.

Fase 3: Informe y Emisión del Sello

- Los auditores elaboran un informe de auditoría con conformidades y no conformidades.
- Si existen no conformidades, la organización debe presentar un plan de acciones correctivas
- El comité de certificación de la entidad evalúa el expediente completo y decide si emitir o no el Sello

Si todo es conforme, se emite el certificado o sello de confianza digital, con registro de validez pública.

Casos Reales
¿Cómo se ha aplicado?

Caso Habitissimo

Confianza que impulsa ventas

- Empresa: Plataforma de reformas online (Mallorca)
- Certificación: Sello de Confianza Online (2023) – Alineado con RGPD
- Impacto en conversión: +15 % de clientes gracias a mayor seguridad percibida.
- Ventaja competitiva: Destacado frente a rivales sin sello; atrajo grandes constructoras
- Mensaje clave: Un distintivo en tu web convierte dudas en contratos al instante

Caso S2 Grupo

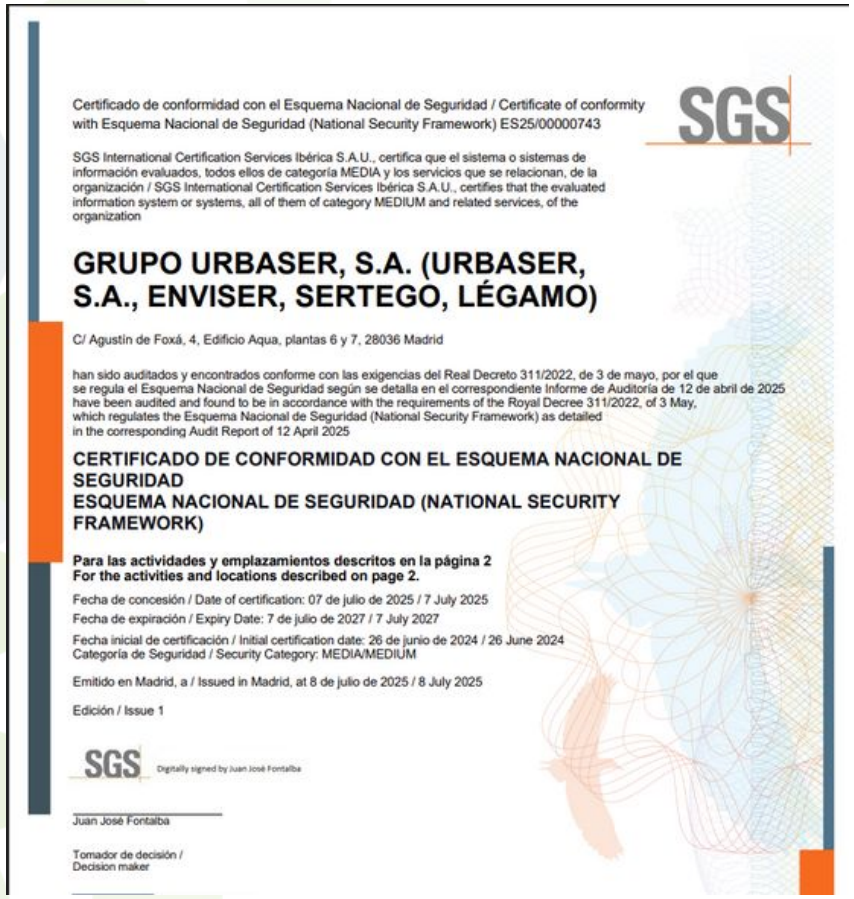
- Empresa: S2 Grupo (Valencia) – Certificaciones ISO 27001 + ENS (2022)
- Acceso a Administración: ENS obligatorio para contratos públicos → contrato cerrado en 2023
- Reducción de riesgos: Incidentes tras implementar mejoras
- Reputación: Reconocidos como referentes en ciberseguridad
- Expansión: Atracción de clientes internacionales y nuevos mercados
- Mensaje clave: Certificación + mejoras operativas = puerta abierta a oportunidades estratégicas

Caso Wallapop. ¿Qué podrían hacer?

Auditoría Inicial: Escaneo de vulnerabilidades en "Wallapop Envíos" con Nessus Professional (NIS2).

- Seguridad Reforzada: Controles de acceso por roles para moderadores de anuncios y asi evitar filtraciones de datos importantes. (ENS).
- Capacitación: Formación anti-phishing para atención al cliente (NIS2).
- Certificación Externa: ISO/IEC 27001 con pruebas de penetración en la app (CRA).
- Mantenimiento del Sello: Notificación de incidentes en 24h en "Wallapop Protect" (NIS2).

Certificados reales:



Certificado de conformidad con el Esquema Nacional de Seguridad / Certificate of conformity with Esquema Nacional de Seguridad (National Security Framework) ES25/00000743

SGS

SGS International Certification Services Ibérica S.A.U., certifica que el sistema o sistemas de información evaluados, todos ellos de categoría MEDIA y los servicios que se relacionan, de la organización / SGS International Certification Services Ibérica S.A.U., certifies that the evaluated information system or systems, all of them of category MEDIUM and related services, of the organization

GRUPO URBASER, S.A. (URBASER, S.A., ENVISER, SERTEGO, LÉGAMO)

C/ Agustín de Foxá, 4, Edificio Aqua, plantas 6 y 7, 28036 Madrid

han sido auditados y encontrados conforme con las exigencias del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad según se detalla en el correspondiente Informe de Auditoría de 12 de abril de 2025
have been audited and found to be in accordance with the requirements of the Royal Decree 311/2022, of 3 May, which regulates the Esquema Nacional de Seguridad (National Security Framework) as detailed in the corresponding Audit Report of 12 April 2025

CERTIFICADO DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD
ESQUEMA NACIONAL DE SEGURIDAD (NATIONAL SECURITY FRAMEWORK)

Para las actividades y emplazamientos descritos en la página 2
For the activities and locations described on page 2.

Fecha de concesión / Date of certification: 07 de julio de 2025 / 7 July 2025
Fecha de expiración / Expiry Date: 7 de julio de 2027 / 7 July 2027
Fecha inicial de certificación / Initial certification date: 26 de junio de 2024 / 26 June 2024
Categoría de Seguridad / Security Category: MEDIA/MEDIUM

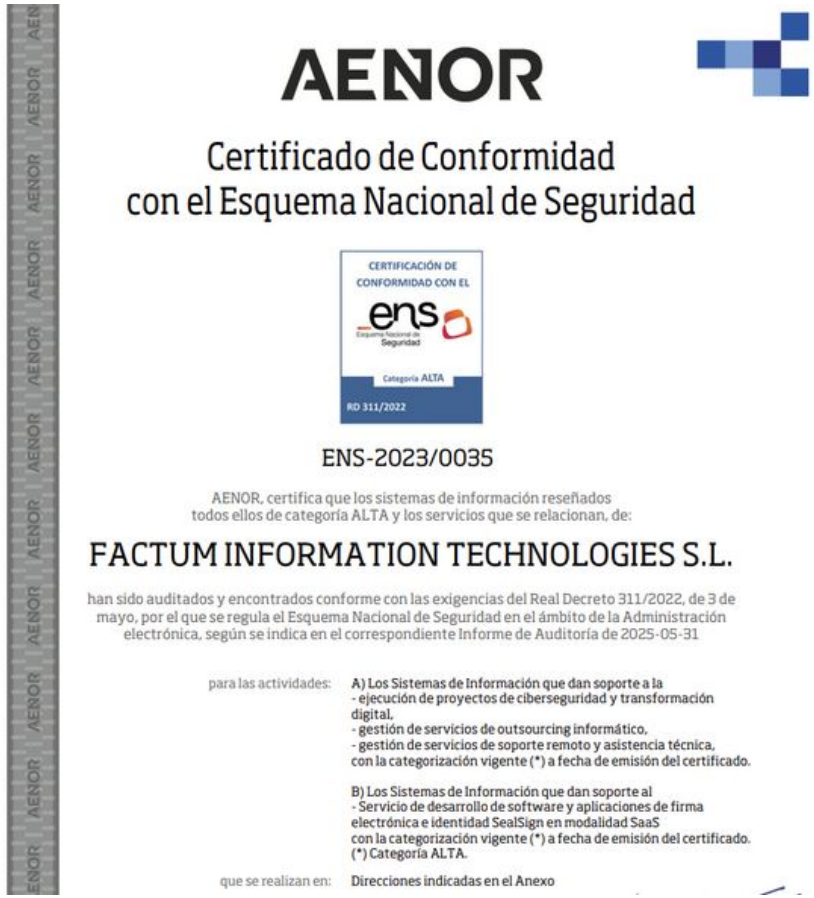
Emitido en Madrid, a / Issued in Madrid, at 8 de julio de 2025 / 8 July 2025

Edición / Issue 1

SGS Digitally signed by Juan José Fontalba

Juan José Fontalba

Tomador de decisión / Decision maker



AENOR

Certificado de Conformidad con el Esquema Nacional de Seguridad

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad
Categoría ALTA
RD 311/2022

ENS-2023/0035

AENOR, certifica que los sistemas de información reseñados todos ellos de categoría ALTA y los servicios que se relacionan, de:

FACTUM INFORMATION TECHNOLOGIES S.L.

han sido auditados y encontrados conforme con las exigencias del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, según se indica en el correspondiente Informe de Auditoría de 2025-05-31

para las actividades: A) Los Sistemas de Información que dan soporte a la
- ejecución de proyectos de ciberseguridad y transformación digital,
- gestión de servicios de outsourcing informático,
- gestión de servicios de soporte remoto y asistencia técnica,
con la categorización vigente (*) a fecha de emisión del certificado.

B) Los Sistemas de Información que dan soporte al
- Servicio de desarrollo de software y aplicaciones de firma electrónica e identidad SealSign en modalidad SaaS
con la categorización vigente (*) a fecha de emisión del certificado.
(*) Categoría ALTA.

que se realizan en: Direcciones indicadas en el Anexo

- Clickable
- Redirección
- Info Detallada
- Actualizado

¿Cómo puedes empezar?

Revisa lo Básico:

Revisa si tu web, correos o sistemas de pago tienen fallos de seguridad

Elige a un responsable:

Pon a alguien de confianza en tu equipo a cargo del proceso

Habla con Todos:

Reúne a tu equipo y explica qué proceso se va a llevar, por qué y posibles expectativas

Organiza tus Datos:

Asegúrate de saber dónde guardas la información de tus clientes y si está protegida

Actualiza lo Básico:

Cambia contraseñas débiles y asegúrate de que tu software esté al día

Reserva tu Cita:

Contacta a una empresa certificadora para empezar el proceso oficial del sello

Certificación tangible: Distintivo verificable que demuestra seguridad a clientes en Salamanca.

Mapeo inicial: Diagnostica riesgos y fortalezas de tus sistemas digitales.

*Auditoría externa: Expertos evalúan y aseguran la calidad de tu ciberseguridad.

Mejoras implementadas: Corrige vulnerabilidades, como software o formación de equipos.

Validación final: Confirma cumplimiento para otorgar el Sello de Confianza.

Cumplimiento normativo

¿Estás listo para certificar tu PYME, O.P y liderar antes de CRA 2027?

Gracias por su atención