AUDITORÍA TÉCNICA DE SOFTWARE

Saber en qué estado está tu sistema, *antes* de decidir sobre él.

Una evaluación independiente de tu sistema y de cómo se construye: **qué tan bien está hecho, qué tan seguro es, cuánto cuesta mantenerlo** y qué conviene corregir primero. Con criterio verificable, no con opiniones.

12
ejes de evaluación, del producto a la operación

10
marcos de referencia internacionales

2
semanas para el primer diagnóstico

0
interrupción de la operación

01 — CUÁNDO SE PIDE

Nadie audita un sistema por *curiosidad*.

Se audita cuando hay una decisión por delante y falta información para tomarla. Estas son las ocho situaciones que más veces la disparan.

01	**Vas a invertir en una nueva etapa de desarrollo** y querés saber si conviene construir sobre lo que hay o empezar de nuevo.
02	**Vas a cambiar de proveedor** y necesitás saber qué estás recibiendo y si podés operarlo sin el anterior.
03	**Vas a comprar una empresa o un producto** y hace falta una revisión técnica previa a la operación.
04	**El sistema anda mal**: se cae, va lento, cada cambio rompe otra cosa, y nadie sabe explicar por qué.
05	**Se fue —o se va a ir— quien lo construyó**, y el conocimiento no está escrito en ninguna parte.
06	**Un cliente grande, una licitación o una certificación** te exige demostrar prácticas de desarrollo y seguridad.
07	**Tuviste un incidente** y necesitás saber si fue un caso aislado o el síntoma de algo más grande.
08	**Estás por escalar** y no sabés si el sistema aguanta el crecimiento que viene.

El servicio no depende del tipo de sistema ni del rubro. Auditamos aplicaciones web, sistemas de gestión, plataformas internas, APIs y aplicaciones móviles, tanto de desarrollo propio como construidas por un tercero.

02 — QUÉ PREGUNTAS RESPONDE

Siete preguntas con respuesta *verificable*.

01	¿Está bien hecho? ¿Contra qué criterio lo estamos diciendo?
02	¿Cuánto cuesta hoy agregarle una funcionalidad nueva, y por qué cuesta eso?

03	¿Qué tan expuesto está, y qué tan probable es que alguien haga algo que no debería?
04	¿Cómo sabemos que un cambio no rompió algo que funcionaba?
05	Si mañana no está quien lo construyó, ¿alguien más puede continuar?
06	¿Sos dueño de tu sistema? ¿Del código, de los datos, de la capacidad de cambiar de proveedor?
07	¿Qué corrijo primero, qué puede esperar, y cuánto cuesta cada cosa?

03 — LOS DOCE EJES

La seguridad es *uno* de los doce ejes.

Y en la mayoría de los sistemas que vemos no es el que más plata está costando. Evaluamos el producto, cómo está construido, cómo se construye y cómo se opera.

BLOQUE A El producto

EJE 01

Adecuación funcional y reglas de negocio

¿Hace lo que el negocio necesita, y lo hace bien?

Cobertura de los procesos reales frente a los que el sistema soporta · reglas de negocio críticas implementadas frente a las documentadas · validaciones y casos borde · consistencia entre lo que muestra la interfaz y lo que queda guardado · cálculos y totales · funcionalidad muerta o duplicada que nadie usa pero todos mantienen.

EJE 02

Experiencia de uso y accesibilidad

¿La gente puede usarlo sin entrenamiento y sin frustrarse?

Recorrido de los flujos críticos y cantidad de pasos reales · claridad de los mensajes de error · errores frecuentes inducidos por el diseño · comportamiento en pantallas chicas · accesibilidad según WCAG 2.2 nivel AA · rendimiento percibido. Un sistema que obliga a un instructivo de tres páginas tiene un problema de diseño, no de capacitación.

EJE 03

Rendimiento y capacidad

¿Aguanta lo que hace hoy y lo que va a hacer en dos años?

Tiempos de respuesta de las operaciones críticas · consultas lentas y consultas repetidas en ciclo · índices faltantes o inútiles · uso de cachés · comportamiento bajo concurrencia · crecimiento proyectado del volumen de datos · límites conocidos y a qué distancia están.

EJE 04

Arquitectura y diseño

¿Se puede cambiar una parte sin romper el resto?

Estructura en capas y separación de responsabilidades · acoplamiento entre módulos y dependencias circulares · puntos únicos de falla · decisiones de diseño registradas y su vigencia · tecnologías elegidas, versiones y estado de soporte · adecuación de la arquitectura al tamaño real del problema, en las dos direcciones: tanto la que quedó chica como la que se sobredimensionó.

BLOQUE B La construcción

EJE 05

Código y mantenibilidad

¿Cuánto cuesta, en horas y en plata, agregar algo nuevo?

Legibilidad y consistencia de convenciones · complejidad de funciones y módulos · duplicación · manejo de errores · dependencias de terceros desactualizadas o con vulnerabilidades conocidas · **licencias de esas dependencias** y su compatibilidad con el uso que les estás dando · deuda técnica identificada, cuantificada y priorizada, no sólo mencionada.

EJE 06

Desarrollo seguro

¿La seguridad está en el proceso o se agrega al final?

Autenticación y gestión de sesiones · control de acceso vertical y horizontal · validación de entradas e inyección · gestión de secretos y credenciales embebidas en el código · cifrado en tránsito y en reposo · exposición de datos en respuestas, direcciones y registros · análisis de composición de dependencias y análisis estático. Evaluado sobre OWASP ASVS y sobre la madurez del proceso según OWASP SAMM.

EJE 07

Datos y modelo

¿Los datos son confiables y se puede reconstruir qué pasó?

Modelo de datos y su correspondencia con el negocio · integridad referencial y restricciones · consistencia y datos huérfanos o duplicados · migraciones, su versionado y su reversibilidad · retención e información histórica · **trazabilidad de los cambios sobre los datos críticos**: quién modificó qué, cuándo y cuál era el valor anterior · calidad de los datos que hoy alimentan reportes y decisiones.

EJE 08

Pruebas y aseguramiento de calidad

¿Cómo sabemos que un cambio no rompió nada?

Existencia y tipo de pruebas automatizadas · cobertura real frente a cobertura útil, que no son lo mismo · pruebas de regresión sobre lo crítico · ambientes de prueba y con qué datos corren · criterios de aceptación · gestión de defectos y cuántos vuelven. La ausencia de pruebas no es un problema estético: es lo que hace que cada cambio sea una apuesta.

BLOQUE C El proceso y la operación

EJE 09

Ingeniería y ciclo de vida

¿Publicar un cambio es un trámite o es un evento?

Control de versiones y estrategia de ramas · revisión de código entre pares · integración y despliegue continuos · nivel de automatización frente a pasos manuales · separación y paridad de ambientes · capacidad efectiva de volver atrás · gestión de cambios y aprobaciones · métricas de entrega: frecuencia de despliegue, tiempo hasta producción, porcentaje de cambios que fallan y tiempo de recuperación.

EJE 10

Documentación y continuidad del conocimiento

¿Si mañana no está quien lo hizo, alguien puede seguir?

Documentación técnica, funcional y de operación, y qué tan vigente está · diagramas que reflejen el sistema actual y no el de hace tres años · guía para poner el proyecto en marcha desde cero · decisiones registradas · **concentración del conocimiento en personas**: cuántas pueden tocar cada parte del sistema, y qué pasa si no están · dependencia efectiva del proveedor.

EJE 11

Infraestructura, operación y observabilidad

¿Nos enteramos de un problema antes que el usuario?

Dónde corre y cómo se aprovisiona · infraestructura descripta como código o configurada a mano · separación de ambientes · gestión de accesos a servidores y servicios · actualizaciones y parches · registros: qué se registra, dónde va y por cuánto tiempo · métricas técnicas y de negocio · alertas y a quién le llegan · proceso de atención de incidentes · costos de operación y si son proporcionales al uso.

EJE 12

Continuidad, cumplimiento y propiedad

¿El sistema es tuyo, y podés seguir sin nosotros y sin ellos?

Respaldos y **evidencia de una restauración probada**, que no es lo mismo que tener backups · plan de recuperación y tiempos objetivo · tratamiento de datos personales conforme a la Ley 25.326 · licencias del software de terceros · **propiedad del código, de los datos y de las cuentas de infraestructura** · contratos con el proveedor · capacidad real de cambiar de proveedor sin rehacer el sistema.

04 — MARCOS DE REFERENCIA

Un hallazgo no es una *opinión*.

Cada hallazgo se referencia a un estándar reconocido. Esa es la diferencia entre una auditoría y un parecer: no es «a nosotros no nos gusta cómo está hecho», es un desvío medible respecto de un criterio que existe fuera de nosotros y que tu equipo puede consultar.

DIMENSIÓN	MARCO DE REFERENCIA
Calidad del producto de software	ISO/IEC 25010 — las ocho características de calidad
Calidad del código fuente	ISO/IEC 5055 (CISQ) — fiabilidad, seguridad, eficiencia y mantenibilidad
Madurez del desarrollo seguro	OWASP SAMM · NIST SP 800-218 (SSDF)
Verificación de la aplicación	OWASP ASVS 4.0 · OWASP Top 10 · API Security Top 10
Procesos del ciclo de vida	ISO/IEC 12207
Rendimiento de la práctica de ingeniería	Métricas DORA
Accesibilidad	WCAG 2.2 nivel AA
Seguridad de la información e infraestructura	ISO/IEC 27001:2022 · CIS Controls v8.1
Gobierno y gestión de TI	COBIT 2019
Protección de datos personales	Ley 25.326 y normativa de la AAIP

> Es una **evaluación con base en marcos de referencia reconocidos**. No constituye una certificación, una habilitación regulatoria ni una declaración de cumplimiento emitida por autoridad competente.

05 — CÓMO TRABAJAMOS

Ocho etapas, y ninguna sorpresa *al final*.

ETAPA 1

Relevamiento y cierre de alcance

Reunión inicial, relevamiento del sistema, del equipo y del contexto, y definición de qué ejes se auditan y con qué profundidad. Cierra con un **acta de alcance firmada**: desde ahí, toda ampliación se gestiona como adenda y nadie se lleva sorpresas.

ETAPA 2

Análisis de artefactos

Documentación, diagramas, repositorio y su historial, tablero de tareas y de defectos, tuberías de integración, contratos y acuerdos de servicio. El historial del repositorio dice más sobre cómo se trabaja que cualquier manual de procedimientos.

ETAPA 3

Análisis técnico

Revisión de arquitectura, código, modelo de datos y dependencias. Combinamos **herramientas automatizadas** —análisis estático, composición de dependencias, métricas de complejidad y duplicación— con **revisión manual** de los módulos críticos. Las herramientas encuentran síntomas; el diagnóstico lo hace una persona.

ETAPA 4

Evaluación en ejecución

Pruebas funcionales sobre los procesos críticos, verificación de controles de acceso con usuarios de distintos perfiles, medición de tiempos de respuesta y revisión de accesibilidad. Sobre ambiente de prueba con datos ficticios siempre que sea posible.

ETAPA 5

Entrevistas con el equipo

El proceso no está en el código: está en la gente. Conversamos con quienes desarrollan, prueban, operan y usan el sistema. Es la etapa donde aparece la mitad de los hallazgos que importan.

ETAPA 6

Análisis, clasificación y priorización

Cada hallazgo se documenta con evidencia, se referencia al marco, y se le asigna tipo, criticidad, esfuerzo estimado y prioridad.

ETAPA 7

Validación con el equipo

Presentamos los hallazgos preliminares antes de escribir el informe final. El equipo tiene derecho a aportar contexto, evidencia o descargo, y se incorpora. Evita errores nuestros y hace que el informe llegue a la dirección sin controversias abiertas.

ETAPA 8

Informe y presentación

Entrega de los documentos y reunión de cierre, en dos registros: uno para la dirección y otro para el equipo técnico.

> **Durante la ejecución.** Si detectamos un hallazgo crítico con riesgo inminente, lo avisamos dentro de las **4 horas hábiles** por el canal acordado, con minuta escrita en 24 horas. No esperamos al informe final para contarte que la base está expuesta.

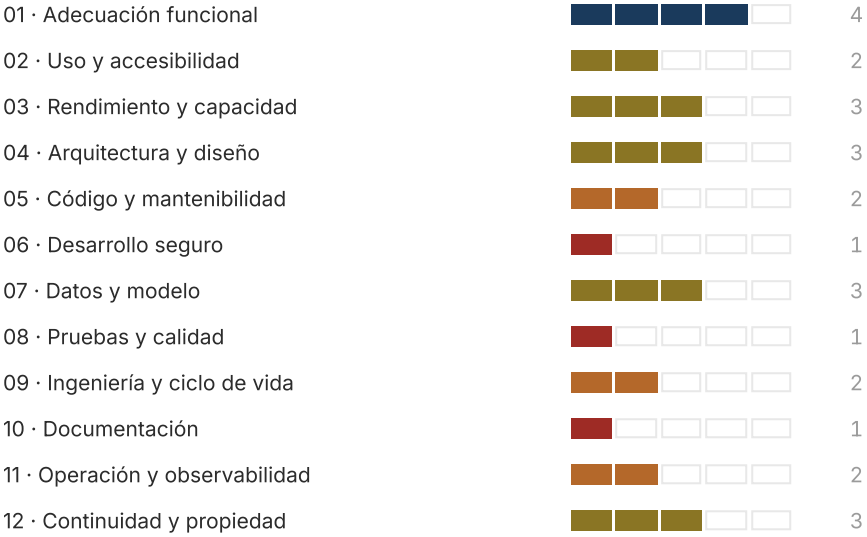
06 — QUÉ RECIBÍS

Siete entregables, y una *hoja de ruta*.

ENTREGABLE	CONTENIDO
Informe ejecutivo	Estado general, riesgos principales, hallazgos críticos y decisiones que requieren dirección. Máximo 10 páginas, sin jerga técnica.
Informe técnico	Hallazgos completos por eje, con evidencia, análisis, referencia al marco y recomendación concreta.
Perfil de madurez	Nivel alcanzado en cada uno de los doce ejes, en una escala de 0 a 5. Permite comparar contra una reauditoría posterior y mostrar avance.
Matriz de hallazgos	Priorizada y filtrable: tipo, criticidad, esfuerzo, prioridad, responsable sugerido y plazo.
Estimación de deuda técnica	Cuánto esfuerzo acumulado hay que invertir para llevar el sistema a un estado sostenible, y qué parte conviene pagar ahora.
Plan de remediación	Agrupado en 0–30, 30–90 y 90–180 días, con esfuerzo estimado, dependencias y ganancias rápidas identificadas.
Presentación de cierre	Una sesión de 60 a 90 minutos, con espacio para preguntas del equipo.

PERFIL DE MADUREZ

EJEMPLO ILUSTRATIVO DEL FORMATO DE SALIDA



NIVEL	ESTADO	QUÉ SIGNIFICA
0	**Inexistente**	La práctica no existe.
1	**Inicial**	Ocurre, pero depende de la iniciativa de una persona.
2	**Repetible**	Se hace de forma parecida cada vez, sin estar escrito.
3	**Definido**	Está documentado y el equipo lo sigue.
4	**Gestionado**	Se mide, y las desviaciones se detectan y corrigen.
5	**Optimizado**	Se mejora de manera deliberada y continua.

> *Llegar a 3 en todo es mejor negocio que llegar a 5 en uno.*

07 — HALLAZGOS Y CRITICIDAD

No todo lo que encontramos es *urgente*.

Cada hallazgo lleva un tipo y una criticidad, porque un defecto funcional, una deuda técnica y un desvío de buena práctica no se atienden igual ni los resuelve la misma persona.

TIPO

TIPO	QUÉ ES
Defecto	El sistema hace algo incorrecto hoy. Se puede reproducir.
Vulnerabilidad	Una debilidad explotable que compromete datos, accesos o disponibilidad.
Riesgo	Todavía no pasó nada, pero las condiciones para que pase están dadas.
Deuda técnica	Funciona, pero encarece cada cambio futuro. Tiene costo aunque nadie lo vea.
Desvío de buena práctica	Se aparta de un estándar reconocido sin una razón documentada.
Oportunidad de mejora	No hay nada mal; hay algo que se puede hacer mejor.

CRITICIDAD

NIVEL	DEFINICIÓN	PLAZO
● Crítico	Riesgo inmediato sobre la información, la seguridad o la continuidad del servicio.	Inmediato
● Alto	Impacto severo, con condiciones acotadas para materializarse.	0–30 días
● Medio	Debilidad que debe corregirse dentro de un plan de mejora.	30–90 días
● Bajo	Riesgo menor o desvío respecto de una buena práctica.	90–180 días
● Observación	No es una falla; requiere atención o una decisión del negocio.	A definir

PRIORIZACIÓN: ESFUERZO FRENTE A IMPACTO

La criticidad dice qué tan grave es. Esta matriz dice **por dónde empezar**, que no siempre es lo mismo.

	ESFUERZO BAJO	ESFUERZO ALTO
Impacto alto	**Ganancias rápidas** Primeros 30 días. Justifican la auditoría solas.	**Proyectos** Se planifican, se presupuestan y se ejecutan por etapas.
Impacto bajo	**Relleno** Se resuelven dentro del trabajo cotidiano.	**Postergables** Se documentan y se aceptan como riesgo asumido.

08 — ALCANCES

Cuatro niveles de *profundidad*.

El precio es fijo por alcance: no se factura por hora incurrida. Las horas indicadas dimensionan el esfuerzo y sirven de base para cotizar ampliaciones.

	ALCANCE 1 Diagnóstico técnico	ALCANCE 2 Auditoría de desarrollo EL MÁS CONTRATADO	ALCANCE 3 Auditoría integral	ALCANCE 4 Integral + acompañamiento
Horas profesionales	40	90	180	180 + 120
Plazo	2 semanas	4 semanas	8 semanas	8 sem. + 12 meses
Para qué sirve	Saber en qué estado estás antes de decidir nada.	Saber si podés seguir construyendo sobre lo que hay.	Sistema crítico del negocio o exigencia de un tercero.	Auditar y además cerrar los hallazgos durante el año.
Ejes cubiertos	Los 12, en superficie	Ejes 4 a 10, en profundidad	Los 12, en profundidad	Los 12, en profundidad
Entrevistas con el equipo	2	4 a 6	6 a 10	6 a 10
Análisis automatizado de código y dependencias	Sí	Sí	Sí	Sí
Revisión manual de código	Muestra	Módulos críticos	Módulos críticos	Módulos críticos
Arquitectura, datos y proceso de ingeniería	Superficial	Completo	Completo	Completo
Desarrollo seguro (ASVS + SAMM)	Barrido	Completo	Completo	Completo
Funcionalidad, accesibilidad y rendimiento	—	—	Sí	Sí
Infraestructura, operación y observabilidad	—	—	Sí	Sí
Continuidad, cumplimiento y propiedad	—	—	Sí	Sí
Perfil de madurez y matriz de hallazgos	Sí	Sí	Sí	Sí
Estimación de deuda técnica	Orden de magnitud	Detallada	Detallada	Detallada
Acompañamiento y verificación de cierre	—	—	—	10 h/mes · 12 meses
Reauditoría a los 6 meses	—	—	—	Sí
Inversión	USD 2.000	USD 4.100	USD 7.600	USD 12.000

El importe del **Diagnóstico técnico** se acredita al 100 % contra la contratación de un alcance mayor dentro de los 90 días.

SERVICIOS ADICIONALES

SERVICIO	HORAS
Prueba de intrusión externa	40
Prueba de intrusión sobre aplicación autenticada	60
Revisión exhaustiva de código por módulo	24 – 80

SERVICIO	HORAS
Pruebas de carga y capacidad	24 – 40
Auditoría de accesibilidad WCAG 2.2 AA completa	32
Evaluación de impacto en protección de datos personales	32
Simulacro de recuperación ante desastres	24
Capacitación al equipo en desarrollo seguro	8 – 16

CONDICIONES

Importes en dólares estadounidenses, **sin IVA**. Facturación en pesos al tipo de cambio vendedor del Banco de la Nación Argentina del día hábil anterior a cada factura. Pago: 40 % a la firma, 40 % contra informe borrador, 20 % contra informe final. Validez de la oferta: 30 días.

09 — QUÉ NECESITAMOS DE VOS

Nada de esto tiene que estar *perfecto* para empezar.

Si falta la mitad, eso ya es parte del diagnóstico.

QUÉ	DETALLE
Acceso de lectura al repositorio	Código fuente y su historial. El historial importa tanto como el código: muestra cómo se trabaja.
Acceso al tablero de trabajo	Tareas, defectos y su historial, si existe.
Un ambiente de prueba	Con datos ficticios y usuarios de los distintos perfiles.
Acceso de sólo lectura	A la base de datos y a la infraestructura, controlado y con cuentas temporales creadas a tal efecto.
La documentación que exista	Diagramas, manuales, decisiones, contratos con el proveedor.
Tiempo del equipo	Entre 4 y 8 horas en total, repartidas en entrevistas cortas.
Un contacto único	Que coordine y reciba los avisos de hallazgo crítico.
Autorización formal firmada	Por quien tenga facultades sobre los sistemas. Define qué podemos revisar, cómo y cuándo.

No pedimos contraseñas personales ni credenciales administrativas existentes. Se crean cuentas temporales, nominadas, de privilegio mínimo y con fecha de vencimiento, que se dan de baja al cerrar.

Firmamos acuerdo de confidencialidad **antes** de ver nada. Tu código no se sube a servicios de terceros ni se procesa fuera de nuestro entorno controlado.

10 — QUÉ NO HACEMOS

Los límites, *por escrito*.

- **No corregimos lo que encontramos.** Recomendamos y acompañamos, pero la ejecución la hace tu equipo o tu proveedor. Es lo que mantiene la auditoría independiente.
- No es una prueba de intrusión. Se cotiza aparte y requiere reglas de compromiso firmadas.
- No hacemos ingeniería social ni pruebas sobre personas.
- No hacemos pruebas de denegación de servicio ni de estrés destructivo.
- No auditamos aspectos contables, legales ni de procesos no informatizados.
- No certificamos bajo ninguna norma.
- **No evaluamos personas.** El informe describe el estado del sistema y qué hacer; no dice quién tuvo la culpa.

11 — PREGUNTAS FRECUENTES

Lo que preguntan *siempre*.

¿Interrumpe la operación?

No. El grueso del trabajo es lectura y análisis fuera de línea. Lo que toque ambientes en uso se acuerda por escrito, con ventana y responsable.

¿Hace falta el código fuente?

Para los alcances 2 y 3, sí, con acceso de lectura. Si no está disponible, se puede auditar igual desde afuera con menos profundidad — y el hecho de que no esté disponible ya es, en sí mismo, un hallazgo importante.

¿Y si el sistema lo hizo otro proveedor?

Es el caso más frecuente. Auditamos el producto, no a las personas. El informe está escrito para que puedas compartirlo con ese proveedor y trabajar con él sobre los hallazgos, en lugar de pelearte.

¿Van a decirme que hay que rehacer todo?

No es la conclusión por defecto, y desconfiá de quien la dé rápido. Rehacer suele ser la opción más cara y más riesgosa. Cuando efectivamente la recomendamos, va acompañada de números que la justifican.

¿Sirve si mi sistema es chico?

Sí. El Diagnóstico técnico está pensado exactamente para eso: dos semanas, un panorama completo y una hoja de ruta, sin comprometerte a un proyecto largo.

¿Quién ve el informe?

Sólo las personas que designes por escrito. Se entrega cifrado, con marca de agua por destinatario, y nunca por correo sin cifrar. Un informe de auditoría es el mapa de las debilidades de tu sistema.

¿Después nos pueden ayudar a arreglarlo?

Sí, pero es una decisión tuya y separada de la auditoría. Nunca inflamos un hallazgo para vender la solución, y si terminamos participando de la remediación, la verificación de cierre la firma alguien distinto de quien emitió el hallazgo.

¿Cuánto tarda desde que decidimos avanzar?

La propuesta con alcance y precio cerrados sale en 5 días hábiles desde la reunión inicial. El proyecto arranca cuando están los accesos.

12 — CÓMO EMPEZAMOS

Una reunión de *45 minutos*.

Sin costo y sin compromiso. Contanos qué sistema es, qué decisión tenés por delante y qué te preocupa. Salimos de ahí con una recomendación de alcance concreta — que puede ser perfectamente que todavía no necesitás una auditoría.

guillermo@cuneo.com.ar — CORREO

+54 9 11 2502-6578 — TELÉFONO

www.cuneo.com.ar — WEB

PASO 1

Reunión inicial de 45 minutos y acuerdo de confidencialidad firmado.

PASO 2

Propuesta con alcance, plazo y precio cerrados, en 5 días hábiles.

PASO 3

Arranque contra la habilitación de accesos y la autorización firmada.

Cuneo · Auditoría técnica de software

Desarrollo · Datos · Infraestructura y cloud · Soporte · Auditoría · www.cuneo.com.ar