04.02.-Impreso de notificación de brechas de seguridad

Serenia Capital, S.A

Organización: Serenia
Documento: Impreso de notificación de incidencias de seguridad
Versión / Fecha: V.1.0 — .....

1. Metadatos de la notificación

Tipo de notificación: ☐ Inicial ☐ Adicional ☐ Completa
Referencia interna: .....
Fecha/hora de cumplimentación: ____ / ____ / ______ hh:mm
Persona que completa el formulario (nombre y cargo): .....
Contacto interno (tel / email): .....

2. Identificación y contacto del DPO

Delegado de Protección de Datos (DPO): Auratech Legal Solutions, S.L.P.
Email de contacto (obligatorio): rgpd@auratechlegal.es
Teléfono (si aplica): .....

3. Identificación del Responsable del Tratamiento

Nombre / Razón social: Serenia Capital, S.A
Tipo de organización: ☐ Privada ☐ Pública
CIF / NIF: .....
Dirección completa: .....
Teléfono / Email de contacto: .....

4. Identificación de Encargados/Subencargados implicados

¿Existe encargado/subencargado implicado? ☐ Sí ☐ No
Si Sí, cumplimentar:
Nombre / Razón social: .....

CIF / NIF: .....

Persona de contacto (tel/email): .....

Relación contractual (breve): .....

5. Información temporal y de detección

Fecha/hora de detección: ____ / ____ / ______ hh:mm ☐ Exacta ☐ Estimada

Medio de detección (sistema / informe humano / tercero): .....

Fecha/hora estimada de inicio de la brecha: ____ / ____ / ______ hh:mm ☐ Exacta ☐ Estimada

¿La brecha está resuelta? ☐ Sí (fecha/hora de resolución: ____ / ____ / ____ hh:mm) ☐ No

Si la notificación se presenta >72h, justificación documental de la tardanza: .....

6. Descripción de la brecha

Resumen narrativo (máx. 300 palabras):

Tipo/s (marcar las que procedan): ☐ Confidencialidad ☐ Integridad ☐ Disponibilidad

Modo/materialización: ☐ Hacking ☐ Malware ☐ Ransomware ☐ Phishing ☐ Error humano ☐ Dispositivo perdido/robado ☐ Correo enviado por error ☐ Publicación no intencionada ☐ Exfiltración por tercero ☐ Otra: .....

Contexto: ☐ Interno (no intencionado) ☐ Interno (intencionado) ☐ Externo (no intencionado) ☐ Externo (intencionado)

7. Sistemas y datos afectados

Sistemas afectados (listar):

Categorías de datos comprometidos (marcar):

☐ Identificativos (nombre, DNI) ☐ Contacto (email, teléfono) ☐ Credenciales ☐ Financieros ☐ Laborales ☐ Localización ☐ Salud / Datos sensibles ☐ Menores ☐ Otros: .....

Número aproximado de registros / personas afectadas: .....

Datos cifrados / pseudonimizados afectados? ☐ Sí ☐ No — Si Sí, indicar método y estado de claves: .....

8. Perfil de los interesados afectados

☐ Clientes ☐ Empleados ☐ Proveedores ☐ Usuarios ☐ Pacientes ☐ Menores ☐ Otros: .....

Identificación de colectivos vulnerables (si procede): .....

9. Evaluación preliminar de riesgo y consecuencias

Consecuencias potenciales (marcar): ☐ Fraude económico ☐ Usurpación identidad ☐ Discriminación ☐ Daño reputacional ☐ Daño físico/salud ☐ Otros: .....

Severidad estimada: ☐ Baja ☐ Media ☐ Alta ☐ Muy alta

Justificación de la severidad (breve): .....

10. Medidas adoptadas y plan de mitigación

Medidas inmediatas aplicadas (contención):

Medidas de erradicación en curso / plan:

Medidas de recuperación previstas / RTO / RPO:

Acciones de comunicación previstas (AEPD / interesados / terceros):

11. Decisión sobre notificación

¿Se ha notificado a la Autoridad de Control (AEPD)? ☐ Sí ☐ No ☐ Pendiente

Si Sí: Fecha/hora de notificación ____ / ____ / ____ hh:mm ; Referencia AEPD (si procede): .....

Si No / Pendiente: **Justificación documentada** (riesgo, cifrado, medidas, esfuerzo desproporcionado, etc.): .....

¿Se ha comunicado a los interesados? ☐ Sí ☐ No ☐ Pendiente

Si Sí: Fecha de envío / nº afectados / medio utilizado: .....

Si No: **Justificación conforme art.34.3 RGPD (si aplica):** .....

12. Implicaciones transfronterizas y sectoriales

¿Existen afectados en otros Estados miembros UE? ☐ Sí ☐ No — Si Sí, listar países: .....

¿Requiere comunicación a autoridades sectoriales, INCIBE, CCN-CERT o FCSE? ☐ Sí ☐ No — Si Sí, indicar cuáles y estado: .....

13. Evidencias y documentación adjunta

Listado de evidencias técnicas adjuntas (hashes, logs, capturas, copias forenses):

Informe técnico inicial / informe de análisis forense: ☐ Sí ☐ No — ubicación / referencia: .....

Comunicación a interesados (borrador / copia): ☐ Sí ☐ No

14. Validación y cierre

Persona responsable de la gestión de la brecha (nombre / cargo): .....

Revisión y validación por DPO (rgpd@auratechlegal.es): ☐ Revisado ☐ Pendiente — Fecha: ____ / ____ / ____

Fecha de cierre del expediente: ____ / ____ / ____

Resumen final / lecciones aprendidas (para informe de resolución):

Instrucciones de uso (resumen práctico)

1. Rellenar de forma inmediata el apartado 1–6 al primer indicio.
2. Abrir expediente en el Registro central de Brechas de Serenia y adjuntar este impreso.
3. Documentar cada actualización (quién / cuándo / qué se añadió).
4. Mantener la cadena de custodia de evidencias y conservar copia cifrada del expediente.

Razones y fundamento normativo — explicación detallada campo por campo

A continuación se explica por qué cada bloque/campo está incluido y su fundamento normativo o de guía práctica. Útil para justificar el formulario ante AEPD, auditoría ISO o inspección.

1. Metadatos de la notificación
¿Por qué? Trazabilidad: quién, cuándo y tipo (inicial/completa). (RGPD art. 33, Guía AEPD). **Uso práctico:** seguimiento y validación.

2. Identificación del DPO
¿Por qué? Art. 33 RGPD exige punto de contacto. Guía AEPD pide contacto claro (email). **Uso:** canaliza comunicaciones.

3. Identificación del Responsable
¿Por qué? Obligatorio indicar responsable y contacto (art. 33.3 RGPD). **Uso:** base para requerimientos.

4. Encargados/Subencargados
¿Por qué? Art. 28 RGPD y trazabilidad contractual. **Uso:** coordinar a terceros y responsabilidades.

5. Información temporal y de detección
¿Por qué? Plazo 72h desde conocimiento (art. 33.1 RGPD). Guía AEPD exige justificar tardanzas. **Uso:** verificar cumplimiento de plazos.

6. Descripción de la brecha
¿Por qué? La AEPD requiere naturaleza/vector. **Uso:** base para evaluación de riesgo y comunicación.

7. Sistemas y datos afectados
¿Por qué? Art. 33.3 RGPD: categorías/volumen de datos y nº de interesados; especial atención a art. 9 RGPD y menores. **Uso:** decide notificación.

8. Perfil de los interesados
¿Por qué? Riesgo aumenta por vulnerabilidad del colectivo. **Uso:** ajusta severidad.

9. Evaluación de riesgo
¿Por qué? EDPB/Guía AEPD: valorar riesgo a derechos y libertades. **Uso:** justifica notificación.

10. Medidas y mitigación
¿Por qué? Art. 33.3 RGPD: medidas adoptadas o propuestas. **Uso:** demuestra diligencia.

11. Decisión sobre notificación
¿Por qué? Registrar decisión y soporte (AEPD/interesados). **Uso:** evidencia ante inspección.

12. Implicaciones transfronterizas/sectoriales
¿Por qué? Cooperación entre autoridades (art. 56 y ss.) y normativa sectorial. **Uso:** coordinar actuaciones.

13. Evidencias
¿Por qué? Cadena de custodia y registros forenses. ISO exige registros. **Uso:** análisis/auditoría/actuación policial.

14. Validación y cierre
¿Por qué? Cierre formal, revisión DPO y lecciones aprendidas. ISO/SGSI. **Uso:** expediente completo y mejora continua.

```
```