04.01.-Plan de actuación interna para la detección y gestión de brechas de seguridad

Serenia Capital, S.A

Índice

1. Objeto y alcance

1.1 Finalidad del plan

La finalidad de este plan es establecer un procedimiento claro, homogéneo y verificable para:

- Identificar y clasificar incidentes de seguridad que puedan constituir brechas de datos personales.
- Definir responsabilidades y roles de los distintos actores implicados (responsable, encargados, subencargados, DPO, comité de seguridad, empleados).
- Evaluar el impacto y el riesgo de cada brecha en los derechos y libertades de las personas afectadas.
- Notificar las brechas a la AEPD y, en su caso, a los interesados, en los términos previstos en los arts. 33 y 34 RGPD.
- Registrar y conservar todas las brechas, sean o no notificables, como parte del principio de responsabilidad proactiva.
- Aprender de cada incidente para reforzar las medidas de seguridad y mejorar la resiliencia de la organización frente a futuros riesgos.

En definitiva, este plan busca no solo el cumplimiento normativo, sino también la protección efectiva de la información y la preservación de la confianza de clientes, empleados, proveedores y socios.

1.2 Ámbito de aplicación

Este plan es de aplicación a todas las actividades de tratamiento de datos personales realizadas por Serenia Capital, S.A (en adelante Serenia) con independencia del soporte (físico o digital) y del entorno tecnológico en que se lleven a cabo.

Quedan incluidos:

- Toda la organización y sus áreas de negocio.
- Empleados y colaboradores externos que intervengan en el tratamiento de datos personales.
- Encargados del tratamiento (proveedores y prestadores de servicios) que traten datos personales por cuenta de Serenia.
- Subencargados del tratamiento autorizados por los encargados, quienes deben seguir el mismo procedimiento de notificación.
- Delegado de Protección de Datos (DPO), en su rol de supervisión, asesoramiento y punto de contacto con la AEPD.

El plan será de obligado cumplimiento para todos los actores mencionados, sin excepción. Su incumplimiento podrá considerarse una infracción de las políticas internas de seguridad y, en su caso, del contrato laboral o de prestación de servicios.

2. Figuras implicadas y responsabilidades

La gestión eficaz de una brecha de seguridad exige la identificación clara de las figuras que intervienen y sus responsabilidades. Cada actor tiene funciones diferenciadas que deben quedar documentadas para garantizar la responsabilidad proactiva (art. 5.2 RGPD) y la trazabilidad de todo el proceso.

2.1 Responsable del tratamiento

Serenia, en calidad de responsable del tratamiento, tiene la responsabilidad última de garantizar el cumplimiento del RGPD y la LOPDGDD en materia de gestión de brechas de seguridad.

Sus principales funciones son:

- Implantar y mantener este plan como parte de su sistema de gestión de seguridad y privacidad.
- Asegurar que existan procedimientos documentados de detección, análisis, notificación y registro de brechas.
- Decidir si la brecha debe notificarse a la AEPD y, en su caso, a los interesados (arts. 33 y 34 RGPD).
- Aprobar las comunicaciones externas relacionadas con una brecha (autoridad de control, afectados, medios de comunicación, organismos sectoriales).
- Garantizar la formación del personal en materia de detección y notificación de incidentes.
- Exigir a los encargados/subencargados el cumplimiento de las obligaciones contractuales de seguridad y notificación.

2.2 Encargados y subencargados del tratamiento

Los encargados del tratamiento (proveedores que gestionan datos por cuenta de Serenia) y sus posibles subencargados deberán:

- Notificar sin dilación indebida al responsable cualquier incidente de seguridad que afecte a los datos personales tratados (art. 28.3.f RGPD).
- Facilitar toda la información necesaria para la evaluación, investigación y documentación de la brecha.
- Colaborar en la aplicación de medidas correctivas y de mitigación.
- No notificar directamente a la AEPD o a los afectados, salvo autorización expresa del responsable.

Estos deberes deberán quedar reflejados en el contrato de encargo de tratamiento conforme al art. 28 RGPD.

2.3 Autoridad de control competente

La Agencia Española de Protección de Datos (AEPD) es la autoridad de control competente en España en materia de protección de datos personales.

En relación con las brechas de seguridad:

- Recibe y evalúa las notificaciones presentadas por el responsable (art. 33 RGPD).
- Puede requerir información adicional o medidas correctivas.
- Supervisa que Serenia ha actuado conforme al marco legal y puede abrir procedimientos sancionadores en caso de incumplimiento.
- Coopera con otras autoridades europeas cuando la brecha tenga dimensión transfronteriza (art. 56 RGPD).

La correcta relación con la AEPD exige que Serenia pueda acreditar en todo momento la documentación de las brechas, tanto las notificadas como las no notificables, siguiendo el principio de responsabilidad proactiva.

2.4 Delegado de Protección de Datos (DPO)

Serenia contará, cuando proceda, con un Delegado de Protección de Datos (DPO), figura obligatoria en determinados supuestos (arts. 37-39 RGPD) y recomendable en todos los casos.

El DPO, con correo de contacto dpo@sereniacapital.com , desempeñará las siguientes funciones en relación con la gestión de brechas:

- Supervisar y asesorar sobre el cumplimiento del plan y la normativa aplicable.
- Emitir criterio jurídico y técnico en la evaluación de riesgos de cada brecha.
- Ser punto de contacto directo con la AEPD en caso de notificación (art. 39 RGPD).
- Revisar y validar la documentación de cada brecha en el registro interno.
- Velar por la formación continua del personal en materia de seguridad y protección de datos.

El DPO actuará de manera independiente y reportará directamente a la alta dirección de Serenia..

3. Fase de detección e identificación

La detección temprana y la correcta identificación de un incidente de seguridad son esenciales para minimizar su impacto y garantizar el cumplimiento de los plazos legales de notificación (72 horas, art. 33 RGPD).

3.1 Reconocimiento y preparación

Serenia reconoce que ninguna organización, independientemente de su tamaño, está exenta de incidentes de seguridad. Por ello:

- Todo incidente potencial deberá ser considerado inicialmente como una posible brecha de seguridad de datos personales, hasta que se demuestre lo contrario.
- La organización contará con canales de comunicación internos habilitados (correo específico de seguridad/privacidad o sistema de tickets) para reportar incidentes.
- Los empleados, colaboradores y proveedores deberán estar formados para reconocer señales de incidentes (correos sospechosos, accesos irregulares, errores de sistemas, pérdida de dispositivos, etc.) y reportarlos de inmediato.
- La preparación incluye la existencia de protocolos documentados y responsables designados para recibir y gestionar los reportes.

Cumple con la exigencia del art. 32 RGPD y la Guía INCIBE (detección proactiva como primera fase del ciclo de gestión de brechas).

3.2 Mecanismos y fuentes de detección (internas y externas)

La identificación de un incidente puede provenir de múltiples fuentes internas o externas. Serenia deberá garantizar que todas ellas se recogen y evalúan sistemáticamente.

Fuentes internas:

- Alertas automáticas de sistemas de seguridad: antivirus, EDR, IDS/IPS, cortafuegos, DLP, SIEM.
- Monitorización de red y análisis de logs: sistemas internos de detección de anomalías.
- Controles organizativos: políticas de seguridad (mesa limpia, bloqueo automático de sesión, control de accesos).
- Reportes de usuarios internos: detección manual por parte de empleados o administradores de sistemas.
- Controles físicos: sistemas de acceso a instalaciones, videovigilancia, alarmas de intrusión.

Fuentes externas:

- Proveedores y encargados del tratamiento: notificación inmediata de incidentes detectados en los servicios que prestan a Serenia.
- Clientes o interesados: alertas recibidas por usuarios que detectan anomalías en sus datos o servicios.

- Organismos públicos: comunicaciones de INCIBE, CCN-CERT, Fuerzas y Cuerpos de Seguridad del Estado u otras autoridades sectoriales.
- Medios de comunicación o foros especializados: vulnerabilidades divulgadas públicamente que puedan afectar a Serenia.

Este apartado cumple con lo exigido por ISO 27002 (16.1.2: reporting of information security events) y con las recomendaciones del INCIBE.

3.3 Proceso de identificación y registro inicial

Una vez detectado un posible incidente, se seguirán los siguientes pasos para su identificación y registro:

Recepción del reporte

- El incidente será comunicado al canal interno designado (correo de seguridad/privacidad o herramienta de gestión de incidencias).
- El receptor (responsable de seguridad/privacidad o DPO) confirmará la recepción y abrirá un registro preliminar.

Análisis inicial

Determinar si el incidente implica una posible brecha de seguridad de datos personales según el art. 4.12 RGPD.

Identificar de forma preliminar:

- Naturaleza del incidente (acceso no autorizado, pérdida, alteración, destrucción, etc.).
- Categoría de los sistemas y datos afectados.
- Posible impacto en la confidencialidad, integridad o disponibilidad.

Clasificación preliminar

- Incidente técnico (no afecta a datos personales, seguimiento interno).
- Posible brecha de seguridad (requiere análisis detallado en fases posteriores).

Registro inicial obligatorio

- Todo incidente quedará documentado en el Registro de Brechas de Seguridad (notificables o no).
- El registro inicial incluirá, al menos: fecha, origen de la detección, persona que informa, descripción preliminar y medidas inmediatas adoptadas.

Este procedimiento se ajusta a la Guía de la AEPD (2018), que exige documentar todas las brechas, y a ISO 27001/27701, que requieren trazabilidad desde la detección.

4. Fase de clasificación del incidente

La clasificación del incidente es fundamental para determinar si se trata de una brecha de seguridad en el sentido del RGPD y qué acciones deben emprenderse. Un error en esta fase puede derivar en notificaciones incorrectas (notificar lo que no procede o, peor aún, omitir lo que sí debía notificarse), lo que constituye una de las causas más frecuentes de sanciones de la AEPD.

4.1 Tipos de amenazas y vectores de ataque

Los incidentes pueden originarse por amenazas internas o externas, con vectores de ataque diversos. Serenia deberá identificar y clasificar el incidente conforme a:

- **Amenazas internas:** errores humanos, negligencia, acceso indebido por parte de empleados, configuraciones incorrectas, incumplimiento de políticas de seguridad.
- **Amenazas externas:** ciberataques (malware, phishing, ransomware, denegación de servicio, explotación de vulnerabilidades), robo físico de soportes o dispositivos.

Vectores de ataque más habituales:

- Correo electrónico: phishing, spear phishing, malware en adjuntos.
- Web y aplicaciones: explotación de vulnerabilidades en aplicaciones, inyección SQL, defacement.
- Redes y sistemas: intrusiones, escaneo de puertos, ataques DDoS.
- Dispositivos y soportes físicos: pérdida, robo o acceso no autorizado a portátiles, móviles, USB.
- Ingeniería social: manipulación de usuarios para revelar credenciales o instalar malware.

Este catálogo es coherente con la Guía INCIBE y los controles de ISO 27002 (16.1: gestión de incidentes de seguridad).

4.2 Categorías de sistemas y datos afectados

La clasificación deberá considerar los sistemas comprometidos y la naturaleza de los datos personales afectados:

Sistemas comprometidos: servidores corporativos, bases de datos, servicios cloud, redes internas, dispositivos móviles, sistemas de backup.

Categorías de datos personales:

- Datos identificativos básicos: nombre, dirección, email, teléfono.
- Datos financieros y económicos: cuentas bancarias, tarjetas, facturación.
- Datos de comportamiento o localización: hábitos de uso, geolocalización, historial de navegación.
- Datos sensibles / categoría especial (art. 9 RGPD): salud, biometría, ideología, religión, orientación sexual.

- Datos relativos a menores: especialmente protegidos por normativa española y europea.

El análisis debe ser proporcional: en una pyme de 2 empleados quizás solo se manejan datos identificativos, mientras que en una empresa de 200 puede haber varias categorías críticas (ej. nóminas, clientes, salud).

4.3 Perfil de usuarios afectados

Se debe identificar qué colectivos de personas resultan afectados:

- **Clientes / usuarios:** riesgo reputacional y pérdida de confianza.
- **Empleados y colaboradores:** incluye datos de nóminas, evaluaciones, accesos internos.
- **Proveedores y partners:** datos contractuales o de acceso a sistemas compartidos.
- **Usuarios vulnerables:** menores, personas dependientes o colectivos con necesidades especiales.

El perfil determina el nivel de riesgo: una brecha que afecta a datos de salud de menores será clasificada como alto riesgo, incluso aunque el volumen de registros sea bajo.

4.4 Impacto en datos personales y operatividad

En esta fase Serenia debe evaluar el doble impacto:

Impacto en los datos personales:

- Confidencialidad comprometida (acceso no autorizado).
- Integridad comprometida (alteración o manipulación).
- Disponibilidad comprometida (pérdida temporal o permanente).
- Riesgo de uso indebido (suplantación de identidad, fraude, chantaje).

Impacto en la operatividad de la organización:

- Interrupción de servicios.
- Pérdida de continuidad de negocio.
- Daños reputacionales.
- Posibles sanciones regulatorias.

Esta valoración debe documentarse en cada incidente para justificar la decisión de notificación a la AEPD/interesados (art. 33 y 34 RGPD).

4.5 Tipologías de incidentes comunes

De acuerdo con la AEPD, INCIBE y la práctica habitual, Serenia reconocerá las siguientes tipologías de incidentes que pueden constituir brechas:

Incidentes de confidencialidad:

- Acceso indebido a datos de clientes por personal no autorizado.
- Envío de correos con destinatarios en copia abierta.
- Publicación o fuga de datos en internet.

Incidentes de integridad:

- Alteración indebida de registros en sistemas corporativos.
- Corrupción de bases de datos por fallo técnico o malware.
- Manipulación de información contable o contractual.

Incidentes de disponibilidad:

- Ataque de ransomware que bloquea datos esenciales.
- Caída prolongada de sistemas críticos sin backup accesible.
- Destrucción de soportes físicos (incendio, inundación).

Incidentes de autenticación y acceso:

- Uso indebido de credenciales robadas.
- Fallos en sistemas de control de accesos (ej. biometría).
- Baja de personal no gestionada que mantiene accesos activos.

Este listado combina lo recogido la Guía AEPD y las tipologías técnicas descritas por INCIBE, dando cobertura a incidentes reales y auditables.

5. Fase de consideración de brecha de seguridad

La fase de consideración permite determinar si un incidente de seguridad constituye efectivamente una brecha de seguridad de datos personales en los términos del artículo 4.12 del RGPD, y, en consecuencia, si debe seguirse el procedimiento de notificación regulado en los artículos 33 y 34 del RGPD.

La correcta clasificación en este punto es esencial para justificar, ante una eventual inspección de la AEPD, por qué una brecha fue notificada o no.

5.1 Diferenciación entre incidente de seguridad y brecha RGPD

No todo incidente de seguridad informática constituye una brecha en el sentido del RGPD. Serenia establece los siguientes criterios:

Incidente de seguridad: cualquier evento que compromete la seguridad de sistemas, redes o información corporativa, pero que no afecta a datos personales.

- Ejemplo: caída temporal de un servidor web que no contiene información personal.

Brecha de seguridad de datos personales (art. 4.12 RGPD): todo incidente que ocasione la destrucción, pérdida, alteración accidental o ilícita, o la divulgación o acceso no autorizado a datos personales tratados por la organización.

De este modo, la consideración de brecha RGPD dependerá de dos factores:

- Que el incidente afecte a datos personales (no solo a información corporativa).
- Que pueda suponer un riesgo para los derechos y libertades de las personas físicas.

El resultado de esta fase deberá quedar documentado en el Registro de Brechas de Seguridad, justificando expresamente la decisión de clasificar o no el incidente como brecha RGPD.

5.2 Clasificación (confidencialidad, integridad, disponibilidad)

Una vez determinado que un incidente constituye una brecha en el sentido del RGPD, deberá clasificarse en función del pilar de seguridad comprometido:

Brechas de confidencialidad: acceso o divulgación no autorizada de datos personales.

- Ejemplos: envío de información de clientes a destinatario equivocado; acceso indebido a historias clínicas por personal no autorizado; fuga de datos publicada en internet.

Brechas de integridad: alteración accidental o ilícita de datos personales, que compromete su exactitud o veracidad.

- Ejemplos: modificación de registros en bases de datos; corrupción de expedientes electrónicos; manipulación fraudulenta de información financiera.

Brechas de disponibilidad: pérdida temporal o definitiva de acceso a datos personales.

- Ejemplos: ataque de ransomware que bloquea el acceso a la base de datos de clientes; fallo en servidores que impide acceder a historiales durante un periodo prolongado; destrucción física de dispositivos de almacenamiento sin copia de seguridad.

Esta clasificación permite determinar el impacto real en los derechos de los afectados y sirve de base para la fase de valoración del alcance.

6. Fase de valoración del alcance

La valoración del alcance tiene como objetivo determinar la gravedad real de la brecha de seguridad y fundamentar la decisión sobre las medidas a adoptar, incluidas las notificaciones legales obligatorias.

Este análisis debe realizarse de manera documentada, objetiva y verificable, atendiendo a criterios técnicos, jurídicos y organizativos.

6.1 Nivel de criticidad de sistemas afectados

Se evaluará la importancia estratégica de los sistemas comprometidos, clasificándolos como:

- **Críticos:** sistemas que contienen información esencial para la continuidad del negocio (bases de datos de clientes, sistemas financieros, sistemas sanitarios, etc.).
- **Muy altos:** sistemas que procesan datos sensibles o de gran volumen.
- **Altos:** sistemas relevantes, pero sin impacto directo sobre procesos críticos.
- **Medios:** sistemas de soporte, cuya afectación genera impacto limitado.
- **Bajos:** sistemas secundarios con información no crítica.

Esta clasificación servirá para priorizar la respuesta y determinar la severidad.

6.2 Naturaleza y sensibilidad de los datos personales comprometidos

Se valorará la tipología de datos afectados, atendiendo a su impacto potencial sobre los derechos de los afectados:

- **Datos básicos identificativos:** nombre, correo, teléfono.
- **Datos de comportamiento:** localización, historial de navegación, hábitos de consumo.
- **Datos financieros:** información bancaria, facturación, tarjetas de crédito.
- **Datos de categorías especiales (art. 9 RGPD):** salud, biometría, ideología, religión, vida sexual.
- **Datos relativos a menores:** con protección reforzada.
- **Datos seudonimizados o cifrados:** menor impacto si las medidas de protección son robustas.

6.3 Severidad de las consecuencias para los interesados

Se analizará el posible efecto sobre los derechos y libertades de las personas afectadas:

- **Baja:** molestias menores (ej. necesidad de restablecer una contraseña).
- **Media:** inconvenientes significativos pero superables (ej. retrasos en servicios, costes económicos moderados).
- **Alta:** consecuencias graves, como fraude financiero, pérdida de empleo o uso indebido de datos sensibles.
- **Muy alta:** consecuencias irreversibles o de larga duración, como exclusión social, daños psicológicos severos, perjuicios para la salud o incluso riesgos vitales.

6.4 Volumen de datos y número de individuos afectados

La magnitud de la brecha se determinará considerando:

- Número de registros afectados.
- Número de individuos identificables.
- Duración de la exposición.

Aunque el número de afectados sea reducido, el riesgo puede ser alto si se trata de datos especialmente sensibles.

6.5 Características especiales de los interesados y responsables

El análisis tendrá en cuenta factores de especial vulnerabilidad:

- **Interesados vulnerables:** menores, personas con discapacidad, colectivos en riesgo de exclusión.
- **Responsable del tratamiento:** el sector en el que opera Serenia puede aumentar el nivel de riesgo (ej. sanidad, banca, educación).

6.6 Impacto en la organización

La brecha puede tener efectos no solo en los afectados, sino también en la propia organización:

- **Operativos:** interrupción de servicios, paralización de procesos.
- **Reputacionales:** pérdida de confianza de clientes, empleados o inversores.
- **Legales y económicos:** posibles sanciones de la AEPD, costes de reclamaciones o litigios.

6.7 Requerimientos legales y regulatorios

En función del análisis anterior, se evaluará si concurren las obligaciones de:

- Notificar a la AEPD en 72 horas (art. 33 RGPD).
- Comunicar a los interesados afectados cuando exista un alto riesgo para sus derechos y libertades (art. 34 RGPD).
- Informar a otras autoridades competentes (INCIBE, CCN-CERT, autoridades sectoriales, Fuerzas y Cuerpos de Seguridad).

Todas las decisiones deberán quedar registradas en el Registro de Brechas de Seguridad, incluyendo la justificación de por qué se notificó o no la brecha a la AEPD y/o a los afectados.

Matriz de valoración de riesgo de brechas de seguridad

Criterio	Nivel bajo	Nivel medio	Nivel alto	Nivel muy alto
Sistemas afectados	Sistemas secundarios sin datos críticos (intranet, apps de soporte)	Sistemas internos con datos operativos no esenciales	Sistemas relevantes (ej. nóminas, CRM de clientes)	Sistemas críticos o core (bases de datos financieras, sanitarias, sistemas centrales)
Naturaleza de los datos personales	Datos básicos identificativos (nombre, email corporativo)	Datos de contacto ampliados, comportamiento o localización	Datos financieros, credenciales de acceso, datos laborales	Datos de categorías especiales (salud, biometría, ideología, menores)
Volumen de datos / nº de afectados	1-10 individuos	11-500 individuos	501-10.000 individuos	Más de 10.000 individuos
Perfil de los afectados	Usuarios internos sin riesgo especial	Empleados y proveedores	Clientes/usuarios externos	Colectivos vulnerables (menores, dependientes, colectivos sensibles)

Consecuencias para los interesados	Molestias menores (restablecer contraseña)	Pérdidas económicas moderadas o retrasos en servicios	Fraude, discriminación, pérdida de empleo, perjuicios financieros graves	Consecuencias irreversibles: daños a la salud, exclusión social, consecuencias vitales
Impacto en la organización	Sin afectación a la continuidad ni reputación	Impacto limitado en procesos internos o reputación	Daños significativos en reputación y continuidad de negocio	Impacto crítico: sanciones graves, pérdida de clientes, crisis reputacional

Uso de la matriz

1. **Asignar** un nivel de riesgo por criterio en cada incidente documentado.
2. **Calcular el nivel global de riesgo:**
   - Si todos los criterios están en "bajo/medio" → **riesgo bajo o moderado**.
   - Si alguno de los criterios es "alto" → **riesgo elevado**.
   - Si alguno de los criterios es "muy alto" → **riesgo crítico**.
3. **Decisión de notificación:**
   - **Riesgo bajo/medio** → se documenta en el registro; puede no ser notificable.
   - **Riesgo alto** → debe notificarse a la AEPD (art. 33 RGPD).
   - **Riesgo muy alto** → además de la AEPD, debe notificarse a los interesados (art. 34 RGPD).

7. Fase de respuesta y mitigación

La respuesta debe ser inmediata, trazable y proporcional al riesgo. Todas las actuaciones quedarán documentadas desde el primer minuto para acreditar responsabilidad proactiva y sustentar las decisiones de notificación.

7.1 Contención

Objetivo: limitar el alcance del incidente, preservar evidencias y evitar nueva exposición.

Medidas mínimas (aplicar según proceda y documentar hora/minuto y responsable):

- **Aislamiento técnico:** desconexión de equipos/sistemas afectados, segmentación de red, bloqueo de IP/dominios/IOC, suspensión de integraciones o colas de procesos que propaguen el incidente.
- **Control de accesos:** revocación/rotación inmediata de credenciales, claves API, certificados y tokens; caducidad de sesiones activas; principio de mínimo privilegio reforzado.
- **Preservación de evidencias:** copia "bit a bit" y salvaguarda de logs (SIEM, firewalls, servidores, aplicaciones, EDR), con cadena de custodia; no formatear ni reinstalar antes de la adquisición forense.
- **Takedown y contención externa:** solicitud de retirada de datos expuestos en repositorios, foros, pastebins o buscadores; coordinación con proveedores cloud y terceros (encargados/subencargados).
- **Comunicación interna operativa:** activación del canal de crisis, designación de portavoz y de un único hilo con el DPO (dpo@sereniacapital.com) para decisiones jurídico-regulatorias.
- **Registro inmediato:** apertura/actualización del expediente en el Registro de Brechas (hechos, medidas urgentes y sistemas afectados).

Resultado esperado: incidente contenido, evidencias preservadas y base documental lista para el análisis.

7.2 Erradicación

Objetivo: eliminar la causa raíz y cualquier persistencia.

Acciones recomendadas:

- **Análisis de causa raíz (técnico y organizativo):** vulnerabilidad explotada, fallo de proceso, ingeniería social, proveedor, configuración. Plan de remediación asociado.
- **Limpieza y desinfección:** herramientas EDR/antimalware actualizadas, escaneo completo, eliminación de artefactos y persistencias; verificación con "hashing"/listas blancas.
- **Gestión de vulnerabilidades y parches:** cierre de CVE, hardening, cambios de configuración; revisión de reglas en WAF/IDS/IPS/DLP/SIEM.
- **Rotación de secretos:** contraseñas, llaves de cifrado, certificados, claves SSH, tokens de servicio e integraciones de terceros.
- **Coordinación con terceros:** encargados/subencargados corrigen su parte y acreditan acciones; actualización del expediente con evidencias de erradicación.
- **Control de cambios:** aplicar en entornos de prueba previos a producción; aprobación por responsable designado y el DPO cuando afecte a datos personales.

Resultado esperado: causa raíz neutralizada y entorno saneado, con evidencia objetiva de erradicación.

7.3 Recuperación

Objetivo: restituir con seguridad los servicios y datos a su estado operativo, evitando reintroducir el riesgo.

Medidas:

- **Restauración segura** desde copias de respaldo verificadas (integridad, punto-en-el-tiempo). Priorizar activos críticos y seguir criterios RTO/RPO.
- **Puesta en producción escalonada:** "canary"/piloto, validaciones funcionales y de seguridad, monitoreo reforzado (detecciones temporales agresivas).
- **Controles compensatorios temporales:** restricciones de acceso, supervisión 24x7, reglas SIEM adicionales, limitación de funcionalidades no esenciales.
- **Comunicación operativa:** instrucciones internas claras para usuarios y equipos; actualización del estado al DPO (dpo@sereniacapital.com).
- **Actualización** del análisis de riesgos y del registro del incidente con la evidencia de recuperación.

Resultado esperado: servicios restablecidos de forma controlada, con verificación de integridad y vigilancia posterior.

7.4 Informe de resolución

Documento final obligatorio para cada expediente, con línea de tiempo y anexos técnicos. **Contenido mínimo:**

- **Hechos y cronología:** detección, contención, erradicación, recuperación; quién hizo qué y cuándo.
- **Sistemas y datos afectados:** categoría de datos personales, volumen estimado, perfil de afectados.
- **Evaluación de impacto y decisión de notificación:** fundamento de la decisión (arts. 33 y 34 RGPD) y, en su caso, copias de las notificaciones realizadas.
- **Medidas adoptadas y eficacia:** qué funcionó, qué no y por qué; evidencias técnicas (hashes, tickets, extractos de logs).
- **Plan de mejora:** acciones preventivas, responsables, plazos y criterios de verificación.
- **Archivo y custodia:** el informe y su expediente se integran en el Registro de Brechas y se conservan, como regla general, durante el plazo interno establecido, con acceso restringido y trazabilidad de consultas.

7.5 Lecciones aprendidas y medidas preventivas

Objetivo: transformar el incidente en mejora del sistema de gestión.

Actividades:

- **Reunión de cierre ("post-incident review")** en ≤10 días laborables desde el restablecimiento, con acta y responsables designados.
- **Revisión de controles y procesos:** endurecimiento de configuraciones, segmentación, MFA, bastionado, segregación de funciones, ciclo de parches, gestión de vulnerabilidades.
- **Refuerzo del factor humano:** programa de formación y simulacros periódicos (phishing tests, ejercicios table-top), con métricas de desempeño y recidiva.
- **Proveedores:** revisión de cláusulas de seguridad y brechas en contratos de encargo; exigencia de evidencias de remediación; evaluación de terceros críticos.
- **Documentación y SGSI:** actualización de políticas/procedimientos, análisis de riesgos, DPIA si cambian los riesgos para los interesados, y plan anual de pruebas. Integración en mejora continua del SGSI (ISO 27001 cl. 10) y del SGPI (ISO 27701).
- **Métricas de aprendizaje (ejemplos):** MTTD/MTTR, número de incidentes por vector, cumplimiento de RTO/RPO, porcentaje de usuarios que superan simulacros, efectividad de parches críticos dentro de SLA.

Resultado esperado: reducción del riesgo residual y aumento de la resiliencia, demostrable ante auditoría, con trazabilidad desde el incidente hasta la mejora implantada.

8. Fase de notificación

La fase de notificación es crítica porque de su correcta ejecución depende el cumplimiento normativo, la transparencia con los afectados y la reducción de sanciones. El RGPD (arts. 33 y 34), la LOPDGDD (art. 32) y la Guía de la AEPD sobre gestión de brechas (2018) establecen que toda brecha debe ser evaluada y, en su caso, notificada en un plazo máximo de 72 horas desde que el responsable tenga conocimiento de ella.

La notificación se compone de tres niveles: comunicación a la autoridad de control, a los interesados y, cuando proceda, a otros organismos públicos con competencias en ciberseguridad o seguridad nacional.

8.1 Notificación a la AEPD (art. 33 RGPD)

- **Plazo legal:** debe realizarse sin dilación indebida y, en cualquier caso, dentro de las 72 horas siguientes a la detección de la brecha.
- **Canal:** la notificación se presentará a través de la sede electrónica de la Agencia Española de Protección de Datos (AEPD), utilizando el formulario oficial de notificación de brechas.

Contenido mínimo (art. 33.3 RGPD):

- Naturaleza de la brecha (categorías y volumen de datos y de interesados afectados).
- Datos de contacto del Delegado de Protección de Datos (dpo@sereniacapital.com o del punto de contacto designado.
- Consecuencias probables de la brecha.
- Medidas adoptadas o propuestas para mitigar los efectos negativos.

Notificación complementaria: si no es posible aportar toda la información en el momento inicial, Serenia deberá presentar una notificación preliminar dentro de las 72 horas y completarla en fases posteriores.

Justificación: si no se realiza notificación, Serenia deberá documentar en el Registro de Brechas las razones objetivas que justifican la decisión, a efectos de inspección por la AEPD.

8.2 Comunicación a los interesados (art. 34 RGPD)

Cuando la brecha suponga un alto riesgo para los derechos y libertades de las personas, Serenia comunicará la incidencia a los interesados sin dilación indebida.

- **Formato y lenguaje:** la comunicación se realizará de manera directa, individual y en un lenguaje claro y comprensible, sin tecnicismos innecesarios.

Contenido mínimo (art. 34.2 RGPD):

- Descripción de la naturaleza de la brecha.
- Consecuencias probables para los interesados.
- Medidas adoptadas por Serenia para mitigar los efectos.
- Recomendaciones sobre las medidas que el interesado puede adoptar para protegerse.
- Datos de contacto del DPO (dpo@sereniacapital.com) para consultas o ejercicio de derechos.

Excepciones (art. 34.3 RGPD): no será necesario comunicar a los interesados si:

- Se aplicaron medidas técnicas (ej. cifrado robusto) que hacen los datos ininteligibles.
- Se han tomado medidas posteriores que eliminan la probabilidad de riesgo.
- La comunicación individual suponga un esfuerzo desproporcionado: en este caso se realizará comunicación pública equivalente.

Registro: toda decisión relativa a la comunicación (realización o excepción) deberá quedar documentada en el expediente del incidente.

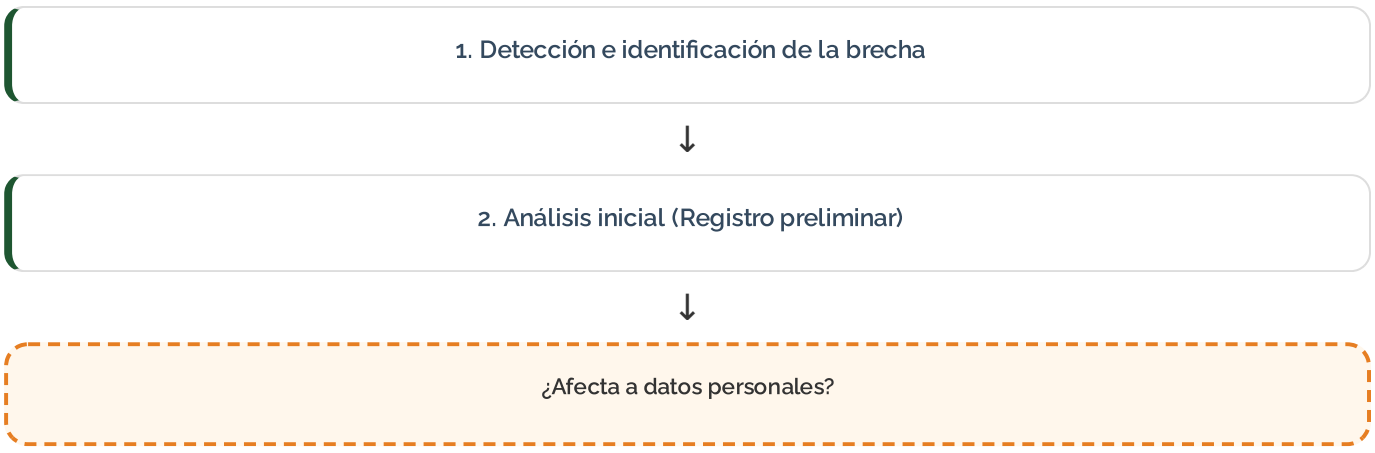
8.3 Comunicación a otros organismos y fuerzas de seguridad

Además de la AEPD y los interesados, en determinados supuestos la brecha deberá comunicarse a otros organismos competentes:

- **INCIBE-CERT:** cuando la brecha implique ciberincidentes relevantes que afecten a la continuidad de negocio o a infraestructuras TIC de la organización.
- **CCN-CERT (Centro Criptológico Nacional):** si la organización forma parte del sector público o gestiona infraestructuras críticas sujetas al Esquema Nacional de Seguridad (ENS).
- **Fuerzas y Cuerpos de Seguridad del Estado (FCSE):** si existen indicios de delito (fraude, extorsión, acceso ilícito, robo de información).
- **Autoridades sectoriales:** organismos reguladores (CNMV, Banco de España, CNMC, autoridades sanitarias) cuando la brecha afecte a sectores regulados.
- **Clientes o socios estratégicos:** cuando contractualmente se haya establecido la obligación de notificación inmediata en caso de incidentes de seguridad.

En todos los casos, la comunicación se realizará de forma coordinada con el DPO (rgpd@auratechlegal.es) y quedará registrada en el expediente de la brecha.

Diagrama de flujo de notificación de brechas de seguridad



No → Incidente de seguridad (*documentar y cerrar*).

Sí → Posible brecha RGPD.

↓

3. Evaluación del riesgo para los derechos y libertades de los afectados

Riesgo improbable → Documentar en el Registro (no se notifica a AEPD ni interesados).

Riesgo probable / significativo → Notificar a la AEPD.

Riesgo alto / muy alto → Notificar a la AEPD + **comunicar a los interesados**.

↓

4. Notificación a la AEPD (art. 33 RGPD)

Plazo máximo: 72 horas.

Contenido: naturaleza de la brecha, datos afectados, consecuencias, medidas adoptadas, contacto del DPO (dpo@sereniacapital.com).

Si falta información → enviar *notificación preliminar* y completarla posteriormente.

↓

5. Comunicación a los interesados (art. 34 RGPD)

Solo si existe **alto riesgo** para sus derechos.

En **lenguaje claro y comprensible**.

Debe incluir: descripción, consecuencias, medidas, recomendaciones y datos de contacto del DPO.

Excepciones: cifrado robusto; medidas posteriores eficaces; esfuerzo desproporcionado (comunicación pública equivalente).

↓

6. Comunicación a otros organismos (cuando proceda)

INCIBE-CERT: ciberincidentes relevantes.

CCN-CERT: sector público o infraestructuras críticas (ENS).

FCSE: indicios de delito (fraude, extorsión, acceso ilícito, robo de información).

Autoridades sectoriales: CNMV, Banco de España, Sanidad, etc.

Clientes o socios: si existe obligación contractual de notificación inmediata.

↓

7. Registro y archivo

Documentar todas las decisiones (notificación o no, plazos, responsables, evidencias).

9. Registro y conservación de las brechas

El registro interno de brechas de seguridad constituye una obligación derivada del principio de responsabilidad proactiva (art. 5.2

RGPD) y del artículo 32 LOPDGDD, así como una práctica exigida por la Guía de la AEPD sobre gestión de brechas de seguridad (2018). Su finalidad es garantizar que Serenia pueda acreditar en todo momento la correcta gestión de los incidentes, tanto si resultaron notificables como si no.

Este registro forma parte integrante del Sistema de Gestión de Seguridad de la Información (SGSI) de la organización y estará a disposición del Delegado de Protección de Datos (dpo@sereniacapital.com), de la dirección y, en caso de inspección, de la AEPD o de otras autoridades competentes.

9.1 Obligación de registro (notificables o no)

- Todas las brechas de seguridad detectadas deberán registrarse, independientemente de que sean notificables o no a la AEPD o a los interesados.
- Este registro permitirá justificar las decisiones adoptadas en relación con la notificación (o su ausencia) y servirá como herramienta para identificar patrones, riesgos recurrentes y necesidades de mejora.
- Los encargados y subencargados del tratamiento estarán obligados a notificar sin dilación indebida al responsable cualquier incidente, de forma que este pueda registrarlo en el sistema centralizado de Serenia.
- En auditoría, se verificará no solo la existencia del registro, sino también la consistencia y trazabilidad de los datos documentados.

9.2 Contenido mínimo del registro

Cada entrada en el Registro de Brechas deberá contener, como mínimo, la siguiente información, conforme al art. 33.5 RGPD y a la Guía AEPD:

Identificación del incidente

- Fecha y hora de detección.
- Fuente de detección (interna/externa).
- Persona que reporta el incidente.

Descripción del incidente

- Naturaleza de la brecha (confidencialidad, integridad, disponibilidad).
- Sistemas y procesos afectados.
- Datos personales comprometidos (categorías y volumen estimado).
- Número aproximado de interesados afectados.

Gestión de la brecha

- Medidas inmediatas de contención.
- Análisis de causa raíz.
- Acciones de erradicación y recuperación aplicadas.

Evaluación del impacto y del riesgo

- Severidad estimada para los derechos y libertades de los afectados.
- Impacto en la organización (operativo, reputacional, legal).

Decisión de notificación

- Determinación de si la brecha es notificable o no.
- Justificación documentada de la decisión.
- Fecha y referencia de la notificación a la AEPD (si aplica).
- Fecha y referencia de la comunicación a los interesados (si aplica).

Cierre del incidente

- Fecha de cierre.
- Informe de resolución vinculado.
- Lecciones aprendidas y medidas de mejora adoptadas.

9.3 Plazos de conservación y medidas de seguridad

Plazos de conservación:

- Los registros se conservarán durante un mínimo de 5 años desde el cierre del incidente, en coherencia con la Guía AEPD y con el plazo de prescripción de las infracciones graves y muy graves en materia de protección de datos (art. 78 LOPDGDD).
- Transcurrido este periodo, la información podrá ser bloqueada y posteriormente eliminada o anonimizada, salvo que exista un procedimiento judicial, administrativo o contractual que justifique su conservación adicional.

Medidas de seguridad:

- El registro deberá almacenarse en repositorios cifrados, con acceso restringido únicamente al DPO, al Responsable de Seguridad y a la dirección.
- Se deberán implementar controles de acceso basados en roles y registrar mediante logs auditables todas las consultas o modificaciones realizadas.
- Se garantizará la integridad y disponibilidad del registro mediante copias de seguridad controladas y almacenadas en entornos seguros.
- En caso de utilización de soluciones cloud, el proveedor deberá ofrecer garantías de cumplimiento normativo (art. 28 RGPD) y contar con certificaciones de seguridad reconocidas (ej. ISO/IEC 27001).

10. Formación, concienciación y simulacros

El factor humano es uno de los vectores de riesgo más relevantes en materia de seguridad de la información. La experiencia demuestra que gran parte de las brechas tienen su origen en errores humanos o técnicas de ingeniería social. Por ello, la formación y la concienciación constituyen medidas preventivas esenciales, exigidas por el artículo 32 RGPD, la LOPDGDD (art. 32) y las normas ISO/IEC 27001 (cl. 7.2 y 7.3).

10.1 Ingeniería social y factor humano

Se reconoce expresamente que la ingeniería social es uno de los principales vectores de ataque, y que el eslabón más débil suele ser el usuario final.

- Serenia implementará programas de sensibilización específicos contra *phishing*, *vishing*, *smishing*, *pretexting*, manipulación telefónica o presencial, y engaños basados en la confianza.
- Se incluirán medidas de control interno (doble verificación en operaciones sensibles, protocolos anti-fraude, uso obligatorio de MFA) para reducir la exposición al factor humano.

10.2 Programas de formación continua

Todos los empleados, colaboradores y proveedores con acceso a datos personales deberán recibir formación inicial obligatoria en materia de protección de datos y seguridad de la información.

Serenia garantizará la existencia de programas de formación continua, actualizados al menos una vez al año, que incluyan:

- Normativa vigente (RGPD, LOPDGDD, ENS si aplica).
- Procedimientos internos de gestión de brechas.
- Buenas prácticas de seguridad en el puesto de trabajo, acceso remoto, dispositivos móviles y entornos *cloud*.
- Lecciones aprendidas de brechas anteriores y tendencias actuales de ciberamenazas.

La asistencia y superación de estas formaciones quedará registrada y podrá ser requerida en auditoría interna o externa.

10.3 Simulacros periódicos y pruebas de respuesta

Serenia realizará simulacros internos de gestión de incidentes con una periodicidad mínima anual, que permitirán probar la eficacia del plan, evaluar tiempos de respuesta y detectar puntos de mejora.

Los simulacros incluirán:

- Ejercicios prácticos de detección y notificación de brechas.
- Pruebas de ingeniería social controladas (campañas de *phishing* simulado).
- Simulaciones de comunicación interna y externa en caso de crisis.

Tras cada simulacro, se elaborará un informe de resultados con indicadores clave (MTTD – tiempo medio de detección, MTTR – tiempo medio de respuesta, tasa de clics en *phishing* simulado, cumplimiento de plazos de notificación). Estos informes formarán parte del ciclo de mejora continua y serán analizados por la dirección y el DPO (dpo@sereniacapital.com).

11. Revisión, auditoría y mejora continua

El plan debe revisarse de forma periódica para garantizar su eficacia y su adecuación a los cambios normativos, tecnológicos y organizativos. Esta obligación deriva del principio de responsabilidad proactiva (art. 5.2 RGPD) y de las normas ISO/IEC 27001 (cl. 9 y 10) e ISO/IEC 27701.

11.1 Auditorías internas y externas

- En caso de que se den brechas se realizarán auditorías internas periódicas, al menos una vez al año desde que tuvo lugar, para verificar el cumplimiento del plan, la correcta gestión de las brechas registradas y la eficacia de las medidas adoptadas.
- En organizaciones sujetas a certificación ISO 27001/27701, el plan será objeto de revisión durante las auditorías de certificación y seguimiento.
- En caso de incidentes significativos o de cambios regulatorios relevantes, se podrán encargar auditorías extraordinarias a terceros especializados.
- Todas las auditorías generarán un informe con hallazgos, no conformidades y recomendaciones, que se integrará en el ciclo de mejora.

11.2 Actualización periódica del plan

El plan será revisado y actualizado al menos una vez al año, o antes si concurren los siguientes supuestos:

- Cambios relevantes en el marco normativo (RGPD, LOPDGDD, ENS, sectorial).
- Modificaciones en los sistemas, procesos o servicios de Serenia que afecten al tratamiento de datos personales.
- Lecciones aprendidas de brechas reales o simulacros que evidencien deficiencias.

Toda actualización será aprobada por la dirección y validada por el DPO (dpo@sereniacapital.com), documentando los cambios y comunicándolos a empleados y proveedores afectados.

11.3 Integración en el SGSI (ISO 27001 / 27701)

Este plan constituye un procedimiento autónomo de Serenia en materia de gestión de brechas de seguridad y es de obligado cumplimiento conforme al RGPD y la LOPDGDD, independientemente de que la organización disponga o no de certificaciones de seguridad.

En aquellas organizaciones certificadas en ISO/IEC 27001 o que gestionen la seguridad bajo un Sistema de Gestión de Seguridad de la Información (SGSI), este plan se integrará en el marco del SGSI, en particular en los **controles de gestión de incidentes (Anexo A.16 ISO 27001)** y en las **revisiones de riesgos y mejora continua (cláusulas 9 y 10)**.

En organizaciones con ISO/IEC 27701, este plan se alineará con los requisitos específicos sobre **violaciones de datos personales (cláusula 6.13)**.

En las organizaciones que no dispongan de un SGSI formal, el presente plan seguirá siendo plenamente válido como procedimiento independiente, garantizando el cumplimiento normativo en materia de protección de datos y seguridad de la información.

Madrid a 3 de octubre de 2025