// MEDIDAS DE SEGURIDAD

Serenia Capital, S.A

ÍNDICE DE CONTENIDOS

Este documento detalla las medidas de seguridad físicas, técnicas y organizativas que Serenia Capital, S.A (en adelante, Serenia) aplica para prevenir la alteración, pérdida, tratamiento o acceso no autorizado a los datos personales tratados en el desarrollo de su actividad, especialmente en los procesos de captación comercial, formularios web, CRM, gestión de expedientes de clientes, tasación de inmuebles, formalización contractual, pagos, atención postventa, gestión de proveedores y cumplimiento normativo. Estas medidas se adoptan de conformidad con el Reglamento (UE) 2016/679 (RGPD), la LOPDGDD y demás normativa aplicable, bajo un enfoque de riesgo, confidencialidad, integridad, disponibilidad, minimización y trazabilidad.

SOPORTE AUTOMATIZADO

1. Medidas Generales

1. **Política de Seguridad de la Información:** Serenia mantiene una política de seguridad de la información documentada, revisada al menos con periodicidad anual o cuando se produzcan cambios relevantes en el tratamiento, en la infraestructura tecnológica o en el nivel de riesgo. Dicha política incluye principios de clasificación de la información, control de accesos, gestión de incidentes, continuidad, teletrabajo, uso aceptable de sistemas y relación con terceros, alineándose con los principios del RGPD y con buenas prácticas basadas en ISO/IEC 27001 y 27002.
2. **Gestión de Activos y Datos:** Se mantiene inventario razonablemente actualizado de activos, aplicaciones, expedientes, repositorios documentales, buzones, dispositivos y servicios cloud utilizados en la actividad de Serenia. La información se clasifica según su sensibilidad y criticidad, distinguiendo entre datos identificativos y de contacto, información económica y patrimonial, documentación contractual, información sucesoria y, cuando proceda, datos de salud o documentación clínica aportada voluntariamente, aplicando controles reforzados a las categorías de mayor riesgo.
3. **Protección contra Malware:** Los equipos y entornos de trabajo utilizados por Serenia disponen de soluciones de protección frente a malware, antimalware y otras amenazas actualizadas, así como mecanismos de actualización periódica del sistema operativo y aplicaciones. Se limita la ejecución de software no autorizado y se promueve el uso exclusivo de herramientas aprobadas por la organización.
4. **Continuidad del Negocio:** Se aplican medidas de continuidad y recuperación proporcionadas al tamaño de la organización, a la naturaleza de sus tratamientos y a la dependencia de servicios cloud, web, CRM, correo electrónico, repositorios documentales y herramientas de gestión. Estas medidas contemplan copias de seguridad, alternativas operativas, restauración de servicios esenciales y gestión de incidentes que afecten a la disponibilidad de la información.
5. **Tratamiento de Archivos Temporales:** Los archivos temporales, borradores, exportaciones, adjuntos y documentos de trabajo que contengan datos personales quedan sujetos a las mismas medidas de seguridad que la documentación definitiva, especialmente cuando incluyan información económica, contractual, bancaria, inmobiliaria, sucesoria o datos sensibles. Se limita su uso, permanencia y duplicación a lo estrictamente necesario.
6. **Uso de Almacenamiento Extraíble:** Se restringe el uso de dispositivos de almacenamiento extraíble para la copia o traslado de datos personales. En caso de uso excepcional por necesidad operativa, el soporte deberá estar cifrado, bajo control del personal autorizado y con devolución o borrado seguro posterior. No se autoriza el uso indiscriminado de soportes personales para documentación de clientes o expedientes.
7. **Gestión de Vulnerabilidades Técnicas:** Se aplican revisiones periódicas de seguridad sobre equipos, aplicaciones, sitios web, formularios, entornos cloud y servicios expuestos a Internet. Se restringe la instalación de software no autorizado, se aplican actualizaciones de seguridad y

1. se revisan las integraciones con terceros, especialmente cuando existan hosting, CRM, herramientas de soporte, formularios web, automatizaciones o proveedores con acceso a datos personales.

2. Política de Seguridad

1. **Establecimiento de Políticas de Seguridad:** Serenia dispone de un marco interno de seguridad que cubre el tratamiento de datos en soporte electrónico, la gestión documental, la relación con proveedores y encargados, la utilización de servicios cloud, el uso del correo electrónico, el acceso remoto y la protección de expedientes comerciales, contractuales y postcontractuales. Estas políticas se aplican también a los tratamientos desarrollados con colaboración de terceros, partners, tasadores, asesorías, hosting, CRM, soporte web y demás proveedores que intervengan en la operativa.

2. **Política de Seguridad y Código de Conducta para Usuarios Internos:** Las personas con acceso a datos personales reciben instrucciones de seguridad, confidencialidad y uso aceptable de sistemas, incluyendo obligaciones sobre contraseñas, correo electrónico, documentación compartida, teletrabajo, impresión, destrucción documental, uso de dispositivos, notificación de incidencias y prohibición de uso no autorizado de la información. Estas obligaciones se refuerzan mediante compromisos de confidencialidad y, cuando proceda, documentación interna o contractual firmada.

3. **Gestión de Eventos de Seguridad:** Se exige la comunicación inmediata de cualquier evento de seguridad que pueda afectar a datos personales, incluyendo accesos indebidos, extravío de documentación, errores de envío, infección por malware, compromisos de credenciales, incidentes en proveedores, indisponibilidad de sistemas, brechas de confidencialidad o integridad y cualquier otra circunstancia con impacto potencial en los derechos de las personas afectadas.

4. **Organización Interna de la Seguridad de la Información:** La organización define responsabilidades internas de gestión de privacidad y seguridad, escalado de incidencias, control de terceros, validación de accesos, aprobación de herramientas y revisión de permisos. En la medida aplicable, se implanta segregación de funciones entre gestión comercial, contratación, pagos, postventa, contabilidad, proveedores y cumplimiento, prestando especial atención a tratamientos de mayor sensibilidad como documentación clínica voluntaria, evaluaciones de longevidad, pagos a herederos, expedientes sucesorios o incidentes de seguridad.

3. Registro de incidencias

1. **Procedimiento de Notificación y Gestión de Incidencias:** Serenia dispone de un procedimiento interno para el registro, análisis, gestión y cierre de incidencias que afecten a datos personales. Este procedimiento contempla, como mínimo, la fecha y hora de detección,

1. el tipo de incidencia, los sistemas o expedientes afectados, la persona que comunica, los efectos detectados, las medidas de contención aplicadas, la evaluación del riesgo y la decisión sobre notificación a la autoridad de control o a las personas afectadas cuando proceda.

2. **Coordinación con Proveedores ante Incidentes:** Los proveedores y encargados del tratamiento con acceso a datos personales deben estar obligados contractualmente a comunicar sin dilación indebida cualquier incidente de seguridad, a colaborar en su investigación, a facilitar las evidencias necesarias y a aplicar medidas de restauración y contención. Esta exigencia resulta especialmente relevante para proveedores de hosting, CRM, correo, repositorios documentales, soporte web, software de gestión y terceros que intervengan en expedientes o integraciones tecnológicas.

4. Control de accesos

1. **Política de Control de Accesos:** Serenia aplica una política de control de accesos basada en el principio de necesidad de conocer y en perfiles autorizados. Los accesos se limitan a las funciones necesarias para cada rol, distinguiendo entre personal de gestión comercial, administración, dirección, asesoría, soporte, proveedores y terceros autorizados. Se contemplan altas, bajas, cambios de rol, revisiones periódicas de permisos y retirada inmediata de accesos cuando dejan de ser necesarios.

2. **Relación Actualizada de Usuarios y Perfiles:** Se mantiene una relación actualizada de usuarios con acceso a sistemas, repositorios documentales, CRM, buzones compartidos y otros recursos que puedan contener datos personales. Los perfiles de acceso se revisan periódicamente y se adaptan cuando cambian las funciones, finaliza una relación profesional o se detecta un acceso excesivo o no justificado.

3. **Gestión de Autenticación y Contraseñas:** Serenia establece medidas de autenticación proporcionales al riesgo, incluyendo contraseñas robustas, identificadores personales e intransferibles, bloqueo tras intentos fallidos y, cuando el riesgo o el sistema lo justifique, autenticación multifactor, especialmente en accesos privilegiados, servicios cloud, correo corporativo, almacenamiento documental y herramientas con expedientes de clientes.

    - **Longitud y robustez de contraseña:** longitud mínima recomendada de 12 caracteres o, cuando la herramienta no lo permita, el máximo robusto soportado, combinando complejidad suficiente y prohibición de reutilización evidente.
    - **Intentos de acceso:** limitación de intentos fallidos y bloqueo temporal automático del usuario o activación de medidas equivalentes de protección frente a fuerza bruta.
    - **Renovación de credenciales:** revisión y cambio cuando exista sospecha de compromiso, baja de usuario, incidencia, acceso indebido o criterio técnico del sistema, evitando prácticas que degraden la seguridad real.
    - **Bloqueo de sesión:** cierre o bloqueo automático por inactividad en aquellos sistemas que traten datos personales o permitan acceso a expedientes, buzones, CRM o documentación sensible.

1. Los identificadores y credenciales son personales e intransferibles, quedando prohibida su cesión o uso compartido.

2. **Medidas de Seguridad Física y Ambiental:** Se aplican medidas de acceso controlado a las instalaciones, puestos de trabajo y soportes documentales, incluyendo control de llaves, custodia documental, acompañamiento de visitas cuando proceda, escritorio limpio, bloqueo de equipos, ubicación segura de impresoras y protección de dispositivos portátiles. En su caso, estas medidas se complementan con mecanismos de protección física del entorno, cierre de despachos, archivadores con llave y controles de acceso restringido a documentación sensible.

5. Copias de respaldo y recuperación

1. **Administración de Procedimientos de Copias de Respaldo y Recuperación:** Se aplican procedimientos de copia de seguridad adecuados al tipo de sistema y criticidad de la información, especialmente para correo corporativo, repositorios documentales, CRM, expedientes, información contractual, datos económicos y documentación necesaria para la continuidad del negocio. La periodicidad de las copias se define conforme al riesgo y a la frecuencia de actualización de los datos.

2. **Procedimientos para Copias de Respaldo y Recuperación de Datos:** Las copias de seguridad y los procedimientos de restauración se revisan periódicamente para verificar su integridad y utilidad real. Cuando sea técnicamente posible, se realizan comprobaciones de recuperación y restauración, al menos sobre los sistemas o repositorios más críticos para la actividad de Serenia.

6. Gestión de soportes y documentos

1. **Medidas Organizativas para la Separación de Datos:** Se aplican medidas organizativas y lógicas para separar la información según su finalidad y nivel de sensibilidad, evitando accesos innecesarios entre expedientes, tratamientos y categorías de interesados. Esta separación es especialmente relevante para documentación clínica voluntaria, evaluaciones de bienestar y longevidad, información sucesoria, pagos, expedientes de clientes, proveedores y empleados.

2. **Identificación y Acceso a Soportes y Documentos:** Los soportes y documentos con datos personales son identificables y solo accesibles por personal autorizado. Se limita la generación de copias, exportaciones o impresiones a lo estrictamente necesario para la operativa, manteniendo trazabilidad razonable cuando el riesgo del tratamiento lo aconseje.

3. **Transporte de Documentación Sensible:** Cuando sea necesario trasladar documentación con datos personales, se adoptarán medidas para evitar la pérdida, extravío o acceso indebido, incluyendo envío seguro, cifrado en soporte electrónico, protección física del expediente y minimización de la información transportada.

1. **Destrucción o Borrado de Documentos y Soportes:** Los documentos y soportes con datos personales se destruyen o borran de forma segura cuando dejan de ser necesarios o finaliza el plazo de conservación aplicable, impidiendo su recuperación no autorizada. Esta medida se extiende a papel, discos, dispositivos, adjuntos, copias temporales, exportaciones y repositorios de trabajo.

7. Responsable de Seguridad / Coordinación de Privacidad

- La dirección de Serenia, junto con la persona o servicio designado para la coordinación de privacidad y seguridad, supervisa la aplicación de las presentes medidas, atiende incidencias, coordina la relación con asesores o proveedores especializados y canaliza las cuestiones relativas a seguridad de la información y protección de datos.

8. Cifrado de Datos

1. **Prácticas de Cifrado de Datos:** Se prioriza el cifrado de la información en sistemas, dispositivos portátiles, repositorios documentales y copias de seguridad cuando el riesgo del tratamiento, la naturaleza del dato o el canal utilizado lo aconsejen, especialmente para documentación contractual, bancaria, sucesoria, expedientes de clientes y documentación sensible o confidencial.

2. **Comunicaciones Cifradas de Punto a Punto o Equivalentes:** Las comunicaciones que impliquen transmisión de datos personales se realizan mediante canales seguros y cifrados, incluyendo protocolos HTTPS/TLS, servicios cloud con cifrado en tránsito y herramientas corporativas razonablemente seguras. Cuando se compartan documentos sensibles, se aplican medidas adicionales de protección, como enlaces restringidos, contraseñas o cifrado del archivo cuando proceda.

9. Control de acceso

- **Registro de Accesos e Intentos Relevantes:** Cuando la naturaleza del sistema o el riesgo del tratamiento lo justifique, se conservará trazabilidad suficiente de accesos, modificaciones, exportaciones, intentos fallidos o actuaciones relevantes realizadas sobre la información, especialmente en sistemas con expedientes de clientes, datos económicos, documentación contractual, buzones corporativos, repositorios documentales y accesos privilegiados.

10. Copias de respaldo y recuperación

- **Ubicación de las Copias de Respaldo:** Las copias de respaldo o mecanismos equivalentes

- de recuperación se conservan, cuando es posible, en entornos lógicamente separados del entorno principal y con medidas que permitan la restauración de la información, priorizando proveedores o infraestructuras con garantías adecuadas y, cuando proceda, ubicación dentro del Espacio Económico Europeo o bajo mecanismos válidos de transferencia internacional.

11. Telecomunicaciones

- **Cifrado de Datos en Transmisiones:** La transmisión de datos personales mediante redes públicas, acceso remoto o conexiones inalámbricas se realiza utilizando medidas de cifrado y protección adecuadas al riesgo, evitando el intercambio inseguro de información sensible o confidencial por canales no autorizados.

12. Medidas de control

1. **Control y Trazabilidad de Accesos de Usuarios Privilegiados:** Los accesos administrativos, privilegiados o con capacidad de configuración sobre servicios, repositorios, correo, CRM, hosting, formularios o herramientas cloud se restringen, documentan y revisan periódicamente.

2. **Políticas de Uso de Controles Criptográficos:** Se establecen criterios de uso de mecanismos criptográficos en sistemas, dispositivos, copias de seguridad y comunicaciones, atendiendo al nivel de riesgo y a la sensibilidad de la información tratada.

3. **Cláusulas de Secreto y Confidencialidad:** Las personas con acceso a datos personales y los terceros que actúen para Serenia quedan sujetos a obligaciones de secreto, confidencialidad y uso limitado de la información, tanto por vía contractual como mediante políticas internas y compromisos específicos de seguridad.

Fecha de generación: 05 de mayo de 2026