**Informe Técnico de Evaluación de Ciberseguridad y Cumplimiento Normativo del Software del Proveedor**

**1. Resumen Ejecutivo**

Este informe analiza la postura de seguridad del proveedor **proveedor-soft.com** en relación con el desarrollo, provisión y operación de su software. Se identifican deficiencias críticas tanto en controles técnicos como organizativos. Destacan la exposición de servicios con credenciales débiles, el uso de certificados caducados, la publicación de datos sensibles en foros clandestinos y backups accesibles públicamente. El proveedor ha sido sancionado por la AEPD, y no cumple con prácticas clave como la revisión de privilegios, trazabilidad de accesos, ni cifrado en reposo. A pesar de su participación reciente en programas de Bug Bounty, sus controles en seguridad de la cadena de suministro, segregación de datos, y gobernanza de IA son limitados o inexistentes. El nivel de riesgo general es alto, y se requieren medidas urgentes de remediación antes de considerar cualquier uso seguro de sus soluciones software.

**2. Nivel de Riesgo General**

**ALTO (89%)**

**Justificación:**

El proveedor presenta fallos graves en áreas esenciales como seguridad en desarrollo, protección de datos, trazabilidad, y controles de acceso. La exposición de servicios críticos (puerto 3389), filtraciones de credenciales, y un historial de sanciones por mal uso de datos agravan la situación. La falta de segregación de datos por cliente, uso parcial de cifrado, ausencia de SBOM y controles débiles sobre IA elevan aún más el riesgo. Aunque existen signos positivos como su participación en programas de Bug Bounty, estos no compensan las deficiencias estructurales identificadas.

**3. Controles Críticos No Cumplidos o Parcialmente Cumplidos**

1. **Gobernanza y Seguridad del Desarrollo**
   * No existe una metodología formalizada de desarrollo seguro (RS-SD-02).
   * No se realiza revisión periódica de privilegios de desarrolladores (RS-SD-04).
   * No se anonimiza sistemáticamente la información en entornos de preproducción (RS-SD-06).
2. **Gestión de Vulnerabilidades y Trazabilidad**
   * El escaneo de vulnerabilidades no es recurrente ni automatizado (RS-CB-02).
   * No hay trazabilidad de accesos ni logs centralizados (RS-CB-04, RS-CB-05).
   * Certificados TLS caducados en subdominios críticos (OSINT).
3. **Protección de Datos y Cumplimiento RGPD/DORA**
   * Solo existe cifrado en tránsito, sin cobertura completa en almacenamiento o uso (RS-DA-01).
   * No se aplica segregación física de datos por cliente (RS-DA-04).
   * El proveedor ha sido sancionado por la AEPD por uso inadecuado de datos personales.
4. **Controles de Seguridad en IA**
   * No existen mecanismos de monitorización, parcheo seguro o filtrado eficaz de datos en soluciones IA (RS-IA-02, RS-IA-05, RS-IA-06).
   * Ausencia total de evaluación de cumplimiento normativo o certificaciones de IA (RS-IA-08, RS-IA-09).
5. **Seguridad de la Infraestructura y Servicios**
   * Servicios RDP expuestos con credenciales débiles (OSINT).
   * Backups accesibles públicamente con documentación técnica sensible (OSINT).

**4. Recomendaciones Específicas y Priorizadas**

1. **Formalización de la Seguridad en el Ciclo de Vida del Software (Alta Prioridad)**
   * Adoptar una metodología formal de desarrollo seguro (como OWASP SAMM).
   * Incorporar controles de revisión de privilegios, anonimización de datos en preproducción y control de cambios documentado.
2. **Mejora de la Protección de Datos y Cumplimiento Normativo (Alta Prioridad)**
   * Asegurar cifrado de datos en uso y en reposo, con algoritmos actualizados.
   * Establecer segregación lógica o física de datos por cliente.
   * Revisar cumplimiento RGPD, DORA y CRA con asesoramiento legal especializado.
3. **Trazabilidad y Gestión de Vulnerabilidades (Media Prioridad)**
   * Implementar soluciones SIEM o API para entrega automatizada de logs.
   * Establecer un proceso continuo de escaneo, priorización y resolución de vulnerabilidades.
   * Emitir y mantener una SBOM actualizada conforme a CRA.
4. **Gobernanza y Seguridad de Componentes de IA (Media Prioridad)**
   * Establecer políticas para monitorizar, auditar y controlar modelos IA en línea con marcos como ISO 42001.
   * Integrar filtrado de datos, validación de entradas, y control de parches en componentes IA.

**5. Conclusión**

El software del proveedor presenta deficiencias graves de seguridad y cumplimiento. Se desaconseja su adopción hasta que se implementen controles sólidos y verificables en desarrollo, protección de datos y gobernanza técnica.